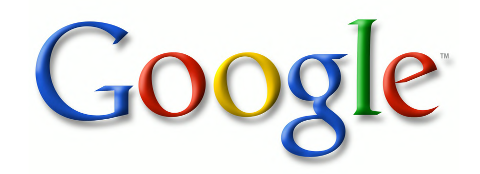
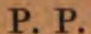




P. P.

Meinen umfangreichen Verlag auf dem Gebiete der **Mathematik** **Technischen-** und **Natur-Wissenschaften** nach allen Richtungen weiter auszubauen, ist mein stetes durch das Vertrauen und Wohlw

u. 272 S.] gr. 8. 1904. ... in Auflage mit eingehender alphabetischer und systematischer Bibliog und einem Gedenktagebuch für Mathematiker. Wünsche um Zuser die kostenfrei erfolgt, nehme ich jederzeit gern entgegen.

Leipzig, Poststraße 3. **B. G. Teubne**

M. V b. 50 : 307.

THEORIE
DER ALGEBRAISCHEN ZAHLEN

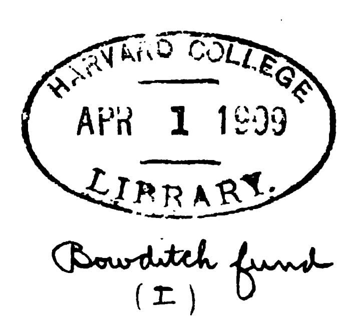
VON

DR. KURT HENSEL

O. Ö. PROFESSOR DER MATHEMATIK AN DER UNIVERSITÄT MARBURG

ERSTER BAND

LEIPZIG UND BERLIN
DRUCK UND VERLAG VON B. G. TEUBNER
1908


HARVARD COLLEGE
APR 1 1909
LIBRARY.

Vorrede.

In dem Werke, dessen ersten Band ich nach achtzehnjähriger Beschäftigung mit diesem Gegenstande der Öffentlichkeit übergebe, behandle ich die Theorie der rationalen und der algebraischen Zahlen nach den Gesichtspunkten, welche die moderne Funktionentheorie mit so gewaltigem Erfolge zur Untersuchung der rationalen und algebraischen Funktionen in ihrem weitesten Umfange benutzt hat.

In der elementaren Arithmetik, wie sie in den „disquisitiones arithmeticae“ von Gauß erst im Anfang des vorigen Jahrhunderts systematisiert und zum Range einer Wissenschaft erhoben worden ist, tritt als Hauptpunkt die Tatsache der Existenz der rationalen Primzahlen und der Satz in den Vordergrund, daß jede rationale Zahl auf eine einzige Weise als Produkt von Primzahlen dargestellt werden kann. Die bahnbrechenden Untersuchungen von Kummer über die algebraischen Zahlen und die auf ihnen sich aufbauenden Betrachtungen von Dedekind und Kronecker gehen genau auf dem von Gauß gewiesenen Wege weiter, und so trat jenen Forschern gleich im Anfang die Schwierigkeit entgegen, daß in diesem höheren Gebiete der Satz von der eindeutigen Zerlegbarkeit der Zahlen in Primzahlen nicht mehr besteht. Hierdurch wurden sie sofort vor die sehr schwere und zunächst fast unlösbar scheinende Aufgabe gestellt, das soeben erst erschlossene Gebiet der algebraischen Zahlen systematisch so zu erweitern, daß in dem neuen größeren Bereiche dieser Fundamentalsatz wieder seine volle Gültigkeit gewinnt. Die Art, wie dieses naturgemäß ganz am Anfang der Untersuchung auftretende schwere Problem von jedem dieser drei Forscher durch eine ihm allein eigentümliche Betrachtung bezwungen wurde, kann wohl als eine ihrer größten wissenschaftlichen Leistungen angesehen werden, und das auf diesem schwer gewonnenen Untergrunde sich erhebende Gebäude der höheren Arithmetik gehört zu den schönsten Ergebnissen, welche die Mathematik der zweiten Hälfte des vorigen Jahrhunderts verdankt.

In der funktionentheoretischen Behandlung der rationalen Funktionen tritt nun der Umstand, daß jede ganze Funktion auf eine einzige Weise in Linearfaktoren zerlegt werden kann, d. h. der Beweis des Gaußschen Fundamentaltheoremes der Algebra, zunächst völlig zurück und ebenso auch der Wunsch, diese Tatsache etwa als Grundlage für die genauere Erkenntnis der Eigenschaften der rationalen und algebraischen Funktionen zu verwenden; dies würde auch schon aus dem Grunde Schwierigkeiten haben, als die Linearfaktoren $z - \alpha$ ja keine eigentlichen Primfaktoren sind, weil sie ebenso wie die Quotienten $\frac{z-\alpha}{z-\beta}$ eine Nullstelle ($z = \alpha$) und einen Pol ($z = \infty$) haben. Dagegen tritt hier die Tatsache in den Vordergrund, daß alle rationalen und algebraischen Funktionen in der Umgebung einer beliebigen Stelle ihres Bereiches, d. h. in der Umgebung eines Punktes der zugehörigen Riemannschen Fläche in Potenzreihen entwickelt werden können, welche nach ganzen oder gebrochenen Potenzen des zugehörigen Linearfaktors fortschreiten, so zwar, daß jeder solchen Stelle ein Zyklus von konjugierten algebraischen Potenzreihen entspricht. Jede zwischen solchen Funktionen bestehende rationale Gleichung bleibt dann für den Bereich einer beliebigen Stelle richtig, wenn man diese Funktionen durch die zugehörigen Funktionenelemente ersetzt. Allein auf dieser Grundlage baut sich dann höchst einfach die Erkenntnis auf, daß die rationalen und die algebraischen Funktionen eindeutige bzw. endlich vieldeutige analytische Funktionen sind, welche nur Pole besitzen. Alle weiteren Ergebnisse, insbesondere der Satz über die eindeutige Zerlegung dieser Funktionen in Primfaktoren und die transzendente Darstellung dieser einfachsten Elemente sind dann verhältnismäßig einfache Folgerungen aus jenem ersten fundamentalen Resultate.

Seit meiner ersten Beschäftigung mit den Fragen der höheren Zahlentheorie glaubte ich, daß die Methoden der Funktionentheorie auch auf dieses Gebiet anwendbar sein müßten, und daß sich auf dieser Grundlage eine in mancher Hinsicht einfachere Theorie der algebraischen Zahlen aufbauen lassen könnte. Die in dieser Richtung geführten Untersuchungen habe ich in dem vorliegenden Werke von den ersten Grundlagen ausgehend so darzustellen versucht, daß sie einen bequemen Eingang in dieses Gebiet gewähren. Die wichtigsten Ergebnisse dieser neuen Zahlenlehre lassen sich kurz folgendermaßen zusammenfassen:

Bei der Untersuchung der rationalen Zahlen in bezug auf ihre Teilbarkeit im weitesten Sinne kann man jeder Primzahl p eine Stelle zuordnen; eine weitere Stelle entspricht dann der Betrachtung dieser Zahlen nach ihrer Größe. Die rationalen Zahlen haben nun die Eigen-

schaft, daß sie für eine jede von diesen Stellen in konvergente Potenzreihen mit rationalen Zahlkoeffizienten entwickelt werden können, welche nach ganzen Potenzen einer zugehörigen rationalen Entwicklungszahl fortschreiten, und welche über die Beziehungen der dargestellten Zahlen zu der betreffenden Primzahl bzw. über alle ihre Größeneigenschaften mit jeder vorgegebenen Genauigkeit Aufschluß geben. Jede rationale Gleichung zwischen rationalen Zahlen bleibt für den Bereich einer beliebigen Stelle richtig, wenn man diese Zahlen durch die zugehörigen Potenzreihen ersetzt.

Die Erweiterung dieser Resultate auf das Gebiet der algebraischen Zahlen ergibt dann die folgenden Resultate: Es sei γ eine beliebige algebraische Zahl n^{ter} Ordnung; wir stellen uns die Aufgabe, die Zahlen des Körpers $K(\gamma)$, d. h. alle rationalen Funktionen von γ mit ganzzahligen Koeffizienten sowohl in bezug auf ihre Teilbarkeitseigenschaften als auch in bezug auf ihre Größe zu untersuchen. Hier ist jeder reellen Primzahl p eine bestimmte Anzahl von Stellen zugeordnet, genau so, wie in der Theorie der algebraischen Funktionen jedem endlichen Werte $z = \alpha$ der unabhängigen Variablen eine Anzahl von Punkten der zugehörigen Riemannschen Fläche entspricht. Alle algebraischen Zahlen des Körpers $K(\gamma)$ haben dann die Eigenschaft, daß sie für den Bereich einer solchen Stelle in konvergente Reihen entwickelt werden können, welche nach ganzen Potenzen einer geeigneten rationalen oder algebraischen Entwicklungszahl fortschreiten und rationale oder algebraische Koeffizienten besitzen. Zu einer und derselben Stelle gehören im allgemeinen mehrere solche Potenzreihen, nämlich der Zyklus aller derjenigen algebraischen Entwicklungen, welche zu einer unter ihnen konjugiert sind. Für den Bereich irgend einer reellen Primzahl p besitzt jede algebraische Zahl unseres Körpers stets n solche voneinander verschiedene Entwicklungen, und diese zerfallen von selbst in so viele Zyklen von konjugierten algebraischen Potenzreihen, als es zu p zugeordnete Stellen gibt. Genau dieselben Betrachtungen gelten auch für die Untersuchung der algebraischen Zahlen nach ihrer Größe; hier existieren so viele verschiedene Stellen, als die Anzahl der unzerlegbaren reellen Faktoren ersten und zweiten Grades beträgt, in welche die linke Seite der Grundgleichung zerfällt, d. h. so viele Stellen als die Anzahl der reellen und der Paare von imaginären Wurzeln jener Gleichung beträgt.

Auch hier besteht der allgemeine Satz, daß die rationalen und die algebraischen Zahlen für den Bereich einer jeden reellen Primzahl und auch ihrer Größe nach eindeutig, bzw. endlich vieldeutig sind, und daß ihre Entwicklungen nur für eine endliche Anzahl von Stellen mit nega-

tiven Potenzen der Entwicklungszahl in endlicher Anzahl beginnen; hieraus folgt dann der Satz, daß jede algebraische Zahl auf eine einzige Weise als ein Produkt von Primteilern dargestellt werden kann.

Jede rationale Gleichung mit rationalen Koeffizienten zwischen beliebig vielen algebraischen Zahlen des Körpers bleibt nun für den Bereich aller Stellen richtig, wenn man die Zahlen durch die ihnen entsprechenden Reihen ersetzt. Jede solche Gleichung repräsentiert einen algebraischen Satz, wenn man die in ihnen auftretenden Zahlen ihrer Größe nach betrachtet, sie ergibt ein arithmetisches Theorem, wenn man diese Zahlen für eine zu einer reellen Primzahl gehörige Stelle untersucht. Bei dieser Auffassung ergibt sich ein vollständiger Parallelismus zwischen den Sätzen über die Größe und denjenigen über die Teilbarkeit der algebraischen Zahlen.

Es sei mir endlich noch gestattet, kurz zu erwähnen, in welchen Punkten die hier entwickelte Theorie der algebraischen Zahlen eine Vereinfachung gegenüber den oben erwähnten ausgezeichneten Darstellungen dieser Disziplin zu ergeben scheint. Fast alle arithmetischen Sätze über die algebraischen Zahlen erhält man hier deshalb ganz besonders einfach, weil man jede von den n zu einer Primzahl p gehörigen Entwicklungen einer algebraischen Zahl isolieren und sie ebenso für sich allein betrachten kann, wie ein einzelnes Element einer algebraischen Funktion in der Umgebung eines Punktes ihrer Riemannschen Fläche; hier braucht man also nicht die zugehörige Gleichung, d. h. die Gesamtheit der n konjugierten Entwicklungen zu betrachten, und ebenso fällt die Bildung und die arithmetische Untersuchung von Resultanten und Diskriminanten fort, wodurch in den andern Theorieen der Überblick mitunter erschwert wird. Ebenso vereinfachen sich die Beweise fast aller hier in Betracht kommenden Sätze und Beziehungen dadurch außerordentlich, daß man ihre Richtigkeit zuerst für den Bereich jeder einzelnen Stelle fast unmittelbar in Evidenz setzen, und dann zeigen kann, daß und wie sie für die Gesamtheit aller Stellen gelten. Endlich erwuchs der allgemeinen Theorie der algebraischen Zahlen dadurch eine beträchtliche in manchen Fällen bisher noch nicht völlig überwundene Schwierigkeit, daß für den gerade betrachteten Körper $K(\gamma)$ gewisse reelle Primzahlen eine Ausnahmestellung einnahmen, so daß die Ergründung ihrer Eigenschaften besondere, nicht immer einfache Untersuchungen nötig machte; es erscheint mir als ein wesentlicher Vorzug der neuen Theorie, daß hier solche Ausnahmen überhaupt nicht auftreten.

In dem vorliegenden ersten Bande wird die allgemeine Theorie der Teilbarkeit der algebraischen Zahlen vollständig entwickelt. An sie schließt sich im Anfange des zweiten Bandes die Untersuchung dieser Zahlen in bezug auf ihre Größe an; die so gewonnenen Resultate sollen dann auf die genaue Untersuchung der besonderen algebraischen Zahlkörper angewendet werden. Die Vorarbeiten für diesen Band sind bereits so weit gediehen, daß seine erste Hälfte bald erscheinen kann.

Bei der Vorbereitung für die Veröffentlichung der ersten Hälfte des vorliegenden Bandes wurde ich durch Herrn Jordan, jetzt Lehrer an der Kotsi-Hochschule in Tsinanfu, in dankenswerter Weise unterstützt, ebenso bei Durchsicht der Druckbogen durch meine verehrten Kollegen Professor Fuëter in Basel und Professor E. Neumann; ihr wertvoller Rat ist mir an manchen Stellen von großem Nutzen gewesen. Ganz besonderen Dank schulde ich Herrn Geheimrat E. Netto, welcher die Druckbogen des ganzen Werkes mit der größten Sorgfalt durchgesehen und mir in schriftlichem und mündlichem Verkehre reiche Anregung für die einfache und klare Darstellung der Theorie gegeben hat. Endlich gilt mein Dank der Verlagsbuchhandlung von B. G. Teubner, die mir meine Arbeit durch verständnisvolles und entgegenkommendes Eingehen auf meine Wünsche wesentlich erleichterte.

Marburg, den 12. Juli 1908.

K. Hensel.

Inhalt des ersten Bandes.

Viertes Kapitel. Seite

Die Zerlegung der ganzen Funktionen mit p-adischen Koeffizienten in ihre irreduktiblen Faktoren.

Fünftes Kapitel.

Untersuchung der algebraischen Zahlen in bezug auf ihre Größe.

Sechstes Kapitel.

Untersuchung der algebraischen Zahlen für den Bereich einer beliebigen Primzahl. Die p-adischen algebraischen Zahlen.

Siebentes Kapitel.

Die Auflösung der ganzzahligen Gleichungen für den Bereich einer beliebigen Primzahl. Theorie der algebraischen Divisoren.

Achtes Kapitel.

Untersuchung der algebraischen Zahlen eines Körpers für den Bereich eines Primdivisors.

Neuntes Kapitel.

Die Darstellung der ganzen algebraischen Zahlen durch ein Fundamentalsystem und die Bestimmung der Körperdiskriminante. — Das zu einem Divisor gehörige Ideal.

Zehntes Kapitel.

Die ganzen algebraischen Zahlen. Die Fundamentalform, die Fundamentalgleichung und die Fundamentaldiskriminante eines Körpers. Die wesentlichen und die außerwesentlichen Diskriminantenteiler. Die gemeinsamen außerwesentlichen Diskriminantenteiler.

Elftes Kapitel.

Die Darstellung der algebraischen Divisoren.

Zwölftes Kapitel.

Die Darstellung der algebraischen Zahlen ihrer Größe nach und für den Bereich einer Primzahl.

Erstes Kapitel.

Die positiven ganzen Zahlen und die elementaren Rechenoperationen.

---

§ 1. Einleitung. Die Methoden der Zahlentheorie und der Funktionentheorie.

Zwischen den beiden größten und wichtigsten Disziplinen der modernen Mathematik, der Funktionentheorie und der Zahlentheorie, besteht bezüglich der Resultate eine sehr merkwürdige und weitgehende Analogie, aber in ihren Methoden eine große Verschiedenheit; und man kann von vornherein sagen, daß eine Vergleichung jener beiden Disziplinen bezüglich der Brauchbarkeit und Wirksamkeit ihrer Methoden sehr wesentlich zu gunsten der Analysis ausfällt.

Die Analysis liefert uns die Mittel, die zu untersuchende Funktion einer komplexen Variabeln in der Umgebung einer jeden Stelle $z = a$ oder $z = \infty$ zu studieren; denn wir sind imstande, das zugehörige Funktionenelement in der Form einer Potenzreihe darzustellen, die in einem Kreis oder Kreisring um den betrachteten Punkt konvergent ist. Wir erhalten so für jede endliche Stelle $z = a$ die Darstellung

$$f(z) = \sum_{\nu} b_{\nu}(z-a)^{\nu},$$

für die unendlich ferne Stelle $z = \infty$

$$f(z) = \sum_{\nu} c_{\nu}\left(\frac{1}{z}\right)^{\nu}.$$

Durch analytische Fortsetzung können wir zwar aus einem Funktionselemente alle anderen herleiten und damit die Eigenschaften der Funktion in der ganzen komplexen Zahlenebene studieren, auch wenn wir nur ein einziges ihrer Elemente kennen. Wenn das jedoch der einzige Weg zur Darstellung der einzelnen Funktionselemente wäre, so würde unsere Funktionentheorie wenig brauchbar sein, obwohl der hohe theoretische Wert dieser Methode nicht zu bestreiten ist. Daher ist es von größter Wichtigkeit, daß wir auch imstande sind, die

einzelnen Funktionselemente unabhängig voneinander zu finden, und zwar ist das immer der Fall, wenn die Funktion durch eine algebraische oder durch eine Differentialgleichung, oder auch durch eine Funktionalgleichung gegeben ist. Auf diesem Wege kommen wir zu voller Einsicht in die Eigenschaften der analytischen Funktionen und gewinnen gleichzeitig vollständige und höchst einfache Kriterien, um die großen Klassen jener Funktionen zu charakterisieren.

Bekanntlich scheiden sich die analytischen Funktionen zunächst in drei große Klassen:

1) Die rationalen Funktionen, welche in der ganzen Ebene eindeutig sind und keine anderen Singularitäten als Pole besitzen.

2) Die algebraischen Funktionen. u ist eine algebraische Funktion von z, wenn u einer algebraischen Gleichung:

$$u^n + g_1(z)\, u^{n-1} + \cdots + g_n(z) = 0$$

genügt, deren Koeffizienten $g_i(z)$ rationale Funktionen von z sind. u ist dann und nur dann eine algebraische Funktion von z, wenn sie endlich vieldeutig ist, und ebenfalls nur polare Unstetigkeiten besitzt.

3) Die transzendenten Funktionen. Eine Funktion u ist dann und nur dann transzendent, wenn sie weder rational, noch algebraisch ist, wenn sie also mindestens eine „wesentlich singuläre Stelle“ besitzt, oder aber unendlich vieldeutig ist. Diese große und wichtige Klasse hat nach dem analytischen Charakter der in ihr enthaltenen Funktionen eine weitgehende Unterteilung erfahren; gerade für die genauere Erkenntnis der transzendenten Funktionen hat die moderne Funktionentheorie das Größte geleistet.

Ganz anders ist dies bei den Zahlen. Auch hier haben wir allerdings eine ganz entsprechende Einteilung, indem wir wiederum drei Klassen unterscheiden:

1) Die rationalen Zahlen. Es sind dies die gewöhnlichen ganzen Zahlen und die Brüche, d. h. die Zahlen, welche sich als Quotienten zweier ganzen Zahlen darstellen lassen.

2) Die algebraischen Zahlen. Eine Größe x ist eine algebraische Zahl, wenn sie Wurzel einer algebraischen Gleichung:

$$x^n + g_1 x^{n-1} + \cdots + g_n = 0$$

ist, deren Koeffizienten ganze oder gebrochene rationale Zahlen sind.

3) Die transzendenten Zahlen. In diese Klasse gehören alle Zahlen, die weder rational noch algebraisch sind.

Die Untersuchungsmethoden für die Zahlen sind nun viel weniger entwickelt als diejenigen für die Funktionen. Es ist allerdings leicht zu bestimmen, ob eine durch einen Dezimalbruch gegebene Zahl

rational ist oder nicht; denn ein unendlicher Dezimalbruch ist dann und nur dann gleich einer rationalen Zahl, wenn er periodisch ist. Dagegen erfordert die Entscheidung, ob eine Zahl algebraisch oder transzendent ist, schwierige Untersuchungen und die Anwendung individueller Methoden für jedes einzelne Problem, während derselbe Nachweis für Funktionen im allgemeinen leicht ist. Daher hat man bis jetzt eigentlich nur für die beiden speziellen Zahlen e und π den Nachweis ihrer Transzendenz geführt. Allgemeine brauchbare Kriterien, um eine Zahl als transzendent zu charakterisieren, gibt es nicht, und wir sind weit entfernt von einer ähnlich genauen Kenntnis dieser Zahlen, wie wir sie bei den transzendenten Funktionen lange besitzen.

Der Grund, warum die allgemeine Untersuchung der Zahlgrößen so außerordentlich viel schwieriger ist als die der Funktionen, scheint mir nun ausschließlich der zu sein, daß wir für die Zahlen im wesentlichen nur eine einzige Darstellung kennen, während wir für jede Funktion unendlich viele Funktionenelemente finden können. Für die Zahlen haben wir nämlich allein die Darstellung ihrer Größe nach, z. B. in Form eines Dezimalbruches mit reellen oder komplexen Koeffizienten. Für eine reelle positive oder negative Zahl besteht nämlich stets die eindeutig bestimmte Entwicklung:

$$C = \pm \sum_{\nu} c_\nu \left(\frac{1}{10}\right)^\nu,$$

wo die c_ν Ziffern aus der Reihe $0, 1, \ldots 9$ sind. Im Fall einer komplexen Zahl $C = A + Bi$ erhalten wir die analoge Darstellung:

$$C = \pm \sum_{\nu} a_\nu \left(\frac{1}{10}\right)^\nu \pm i \sum_{\nu} b_\nu \left(\frac{1}{10}\right)^\nu = \pm \sum_{\nu} (a_\nu \pm i b_\nu) \left(\frac{1}{10}\right)^\nu,$$

wo die Ziffern a_ν und b_ν wieder Zahlen der Reihe $0, 1, \ldots 9$ bedeuten.

Wir haben also für die Zahlen nur die Entwicklung nach fallenden Potenzen von 10 oder, was genau dasselbe ist, von irgend einer anderen Grundzahl; der Form nach entspricht dies der Entwicklung einer analytischen Funktion $f(z)$ nach fallenden Potenzen von z, d. h. in der Umgebung der unendlich fernen Stelle. Die Theorie der Funktionen würde genau dieselben Schwierigkeiten bieten wie die der Zahlen, wenn wir für sie etwa auch nur eine Entwicklung kennen würden, wenn sie z. B. nur in der Umgebung des Nullpunktes oder des unendlich fernen Punktes, also durch eine einzige Potenzreihe $\sum c_i z^i$ gegeben wären und wenn wir daraus alle ihre Nullstellen, Pole usw. finden sollten. Wenn man nun für die Darstellung der Zahlen dieselbe Mannigfaltigkeit erreichen kann, wie sie die Lehre von den Funktionen auszeichnet, so wird man auf dem Wege sein, die

Zahlentheorie zu derselben methodischen Vollkommenheit und leichten Anwendbarkeit zu führen, welche die Funktionentheorie seit den grundlegenden Untersuchungen von Cauchy, Riemann und Weierstraß besitzt. Diese neue Darstellung möchte ich hier von ihren ersten Anfängen an geben. Dabei brauche ich fast nichts an arithmetischen Kenntnissen vorauszusetzen, denn die wenigen Hilfsmittel aus der elementaren Theorie der Zahlen werden wir hier in naturgemäßer Weise selbst herleiten.

§ 2. Die ganzen Zahlen. Primzahlen. Darstellung der ganzen Zahlen für den Bereich einer Primzahl.

Die einzigen Zahlen, welche uns von Natur gegeben sind, sind die ganzen positiven Zahlen. Von diesen gehen wir aus und knüpfen die Erweiterung des Zahlengebietes an sie an. In der elementaren Arithmetik wird gezeigt, daß und wie man die ganzen Zahlen durch die Operationen der Addition und Multiplikation miteinander verbinden kann und daß man durch Anwendung dieser Operationen nicht aus dem Bereich der ganzen Zahlen herausgeführt wird. Für die elementare Zahlentheorie ist die Multiplikation besonders wichtig, da die multiplikativen Eigenschaften der Zahlen sich leicht ermitteln lassen, während die meisten Fragen der additiven Zahlentheorie sehr schwierig sind.

Die erste sich uns darbietende Frage ist die nach den einfachsten Elementen, aus denen sich alle Zahlen multiplikativ zusammensetzen lassen. Sie wird durch den folgenden elementaren Satz beantwortet, der hier nicht mehr bewiesen zu werden braucht:

> Unter den ganzen Zahlen gibt es einfachste Elemente, die Primzahlen:
>
> $$2,\ 3,\ 5,\ 7,\ 11,\ \ldots$$
>
> welche multiplikativ nicht weiter in einfachere Bestandteile zerlegt werden können. Es gibt, wie schon Euklid bewiesen hat, unendlich viele Primzahlen. Jede andere ganze Zahl läßt sich auf eine einzige Weise als Produkt von Primzahlen darstellen.

Unsere nächste Aufgabe ist nun, das Verhalten einer gegebenen Zahl A in bezug auf eine gegebene Primzahl p genau zu ergründen. Es ist zuerst zu untersuchen, durch welche Potenz der Primzahl die gegebene Zahl teilbar ist, d. h. man hat A in der Form $p^{\delta} A_0$ darzustellen, wo A_0 nicht mehr durch p teilbar ist. Hieran schließt sich dann die weitere Untersuchung der Zahl A_0. Diese sowie alle andern hierhergehörigen Fragen werden am einfachsten und naturgemäßesten beantwortet, wenn man sich entschließt, die ganzen Zahlen ebenso nach Potenzen jener Primzahl zu entwickeln, wie man in der Funktionen-

theorie die in der Umgebung einer Stelle $z = a$ zu untersuchende Funktion nach steigenden Potenzen des zugehörigen Linearfaktors $z - a$ entwickelt. Für diese Darstellung gilt der folgende Satz:

> Jede ganze positive Zahl A läßt sich auf eine einzige Weise nach steigenden Potenzen der Primzahl p entwickeln, d. h. in der Form:
>
> (1) $$A = a_0 + a_1 p + a_2 p^2 + \cdots + a_\varrho p^\varrho$$
>
> so darstellen, daß die Koeffizienten a_i eindeutig bestimmte Zahlen der Reihe $0, 1, 2, \cdots (p-1)$ sind.

Diese Entwicklung ist nichts anderes als die Darstellung der Zahlen im p-adischen Zahlensystem, d. h. im System mit der Grundzahl p, und entspricht genau der gewöhnlichen Darstellung der Zahlen im System mit der Grundzahl 10. Die Koeffizienten dieser Entwicklung sind offenbar eindeutig bestimmt; man findet sie am einfachsten durch fortgesetzte Division mit p, indem man das folgende System von Gleichungen bildet:

(2) $$\begin{aligned} A &= a_0 + pA_1, \\ A_1 &= a_1 + pA_2, \\ &\vdots \\ A_{\varrho-1} &= a_{\varrho-1} + pA_\varrho, \\ A_\varrho &= a_\varrho. \end{aligned}$$

Hier bedeutet allgemein a_i den kleinsten nicht negativen Rest, welchen A_i bei der Division durch p läßt. Da die Zahlen $A, A_1, \ldots$ eine abnehmende Reihe bilden, so muß einmal ein Quotient A_ϱ selbst kleiner als p, der nächstfolgende also Null werden, so daß die Reihe nach einer endlichen Anzahl von Divisionen abbricht. Multipliziert man die Gleichungen des Systems (2) sukzessive mit $1, p, p^2 \ldots p^\varrho$ und addiert sie dann, so ergibt sich nach Weglassung der beiderseits auftretenden Glieder $A_i p^i$ die gesuchte Gleichung (1). Zur Erläuterung wollen wir die Zahl 216 nach Potenzen von 5 entwickeln. Wir erhalten dafür die Gleichungen:

$$\begin{aligned} 216 &= 1 + 5 \cdot 43, \\ 43 &= 3 + 5 \cdot 8, \\ 8 &= 3 + 5 \cdot 1, \\ 1 &= 1. \end{aligned}$$

Hieraus ergibt sich die Entwicklung:

$$216 = 1 + 3 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3.$$

Diese Darstellung ist keineswegs auf Primzahlen beschränkt; statt der Primzahl p könnten wir auch jede beliebige andere ganze Zahl

wählen. Wir werden jedoch aus einem später anzugebenden Grunde im folgenden nur die Entwicklungen nach Primzahlpotenzen benutzen.

Die soeben gefundene Gleichung (1) wollen wir die Darstellung von A für den Bereich von p oder als p-adische Zahl nennen. Für jede Zahl A gibt es also ebensoviele verschiedene Darstellungen, als es Primzahlen gibt.

Zur Vereinfachung der Schreibweise bei den folgenden Untersuchungen wollen wir noch einige nützliche Bezeichnungen einführen. Unter den Koeffizienten $a_0, a_1, \ldots$ können gewisse Null sein. Es sei a_α der erste nicht verschwindende Koeffizient, so daß die Entwicklung von A sich in der Form:

$$A = a_\alpha p^\alpha + a_{\alpha+1} p^{\alpha+1} + \cdots + a_\varrho p^\varrho$$

oder

$$A = p^\alpha (a_\alpha + a_{\alpha+1} p + \cdots + a_\varrho p^{\varrho-\alpha})$$

darstellt; d. h. A ist genau durch p^α und durch keine höhere Potenz von p teilbar. Diese Tatsache drücken wir aus mit den Worten „A besitzt in bezug auf p die Ordnungszahl α“. Jede Zahl unseres Bereiches besitzt also in bezug auf eine gegebene Primzahl eine bestimmte Ordnungszahl α, die eine ganze positive Zahl oder Null sein kann.

Eine Zahl

$$E = e_0 + e_1 p + e_2 p^2 + \cdots$$

heißt eine Einheit für den Bereich von p, wenn sie in bezug auf p die Ordnungszahl Null hat, wenn also $e_0 > 0$ ist. Eine Einheit für den Bereich von p ist demnach jede durch p nicht teilbare Zahl. Jede andere Zahl A läßt sich für den Bereich von p auf eine einzige Weise in der Form:

$$A = p^\alpha \cdot E$$

darstellen, d. h. als Produkt einer Einheit und einer Potenz von p, deren Exponent gleich der Ordnungszahl von A ist. Die größte in einer Zahl A enthaltene Potenz von p wollen wir auch den absoluten Betrag von A für den Bereich von p nennen und durch $|A| = p^\alpha$ bezeichnen.

Bildet man aus zwei Zahlen

$$A = p^\alpha E, \qquad B = p^\beta E'$$

das Produkt

$$AB = p^{\alpha+\beta} E E',$$

so findet man, da das Produkt zweier Einheiten offenbar wieder eine Einheit ist, den Satz:

Die Ordnungszahl eines Produktes aus zwei oder mehreren Faktoren ist gleich der Summe der Ordnungszahlen seiner

Faktoren. Oder auch der absolute Betrag eines Produktes ist gleich dem Produkte der absoluten Beträge seiner Faktoren.

Zur leichteren Repräsentation einer p-adischen Zahl

$$A = a_0 + a_1 p + a_2 p^2 + \cdots + a_\varrho p^\varrho$$

will ich nach Analogie der Dezimalbrüche die Darstellung:

$$A = a_0, a_1 a_2 \cdots a_\varrho \quad (p) \tag{3}$$

benutzen, in der allgemein der mit p^k multiplizierte Koeffizient a_k an die k^{te} Stelle hinter dem Komma gesetzt ist; das beigefügte (p) soll angeben, daß die Darstellung für den Bereich von p gilt. So vertreten z. B. die Gleichungen:

$$\begin{aligned} 216 &= 0{,}0011011 \quad (2) \\ &= 0{,}0022 \quad (3) \\ &= 1{,}331 \quad (5) \end{aligned}$$

bzw. die folgenden ausführlichen Gleichungen:

$$\begin{aligned} 216 &= 1 \cdot 2^3 + 1 \cdot 2^4 + 1 \cdot 2^6 + 1 \cdot 2^7 \\ &= 2 \cdot 3^3 + 2 \cdot 3^4 \\ &= 1 + 3 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3. \end{aligned}$$

Die abgekürzte Schreibweise (3) einer Zahl setzt uns auch in den Stand, ihre Ordnung unmittelbar abzulesen, denn diese ist gleich der Anzahl der Nullen, die am Anfang stehen.

§ 3. Die Näherungswerte, die reduzierte und nicht reduzierte Darstellung der Zahlen. Die Addition und Multiplikation.

Bei der Untersuchung einer Zahl A für den Bereich von p kann man meistens von den höheren in ihr auftretenden Potenzen von p, d. h. von ihren späteren Ziffern ebenso absehen, wie man bei einer durch einen Dezimalbruch dargestellten Zahl nur eine gewisse Zahl ihrer Anfangsziffern braucht, d. h. sich mit einem für die Zwecke der jedesmaligen Untersuchung genügend genauen Näherungswerte begnügt. Aus diesem Grunde will ich auch bei unserer Untersuchung **Näherungswerte für den Bereich von p** einführen, und ich definiere dieselben folgendermaßen:

Unter dem k^{ten} Näherungswerte der Zahl

$$A = a_0, a_1 a_2 \cdots a_k a_{k+1} \cdots a_\varrho \tag{1}$$

verstehe ich die Zahl:

$$A_k = a_0, a_1 a_2 \cdots a_k = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k,$$

die ich erhalte, wenn ich in A alle auf a_k folgenden Ziffern weglasse. So ist beispielsweise:

$$A_0 = a_0 \quad A_1 = a_0, a_1 \quad A_2 = a_0, a_1 a_2, \cdots.$$

Wir bekommen so eine wohldefinierte Reihe von Zahlen

$$A_0, A_1, A_2, \cdots A_k \cdots$$

die mit A bzw. in der ersten, den beiden ersten, den drei ersten ... den $(k+1)$ ersten Stellen übereinstimmen und für die allgemein:

$$A_{k+1} = A_k + a_{k+1} p^{k+1}$$

ist. Auch für die Zahl A selbst besteht eine Gleichung:

$$A = A_k + p^{k+1} \bar{A}_k,$$

d. h. sie ist gleich ihrem k^{ten} Näherungswerte, vermehrt um eine Zahl, die mindestens durch p^{k+1} teilbar ist. Die Reihe der Näherungswerte von A bricht mit dem ϱ^{ten} ab. Fügt man aber in der Darstellung (1) von A, was offenbar erlaubt ist, hinter a_ϱ noch beliebig viele Nullen hinzu, so besitzt diese Zahl $a_0, a_1 \ldots a_\varrho 0 0 \ldots$ beliebig viele auf A_ϱ folgende Näherungswerte, welche aber alle mit $A_\varrho = A$ übereinstimmen.

Mit Hilfe des Begriffs der Näherungswerte definieren wir die Kongruenz zweier Zahlen unseres Bereiches auf folgende Weise:

> Zwei Zahlen A und A' heißen **kongruent für den Modul** p^k, wenn ihre $(k-1)^{\text{ten}}$ Näherungswerte für den Bereich von p, also auch alle früheren, übereinstimmen. Man drückt diese Beziehung folgendermaßen aus:
>
> $$A \equiv A' \pmod{p^k}.$$

Schreiben wir A und A' in der Form

$$A = A_{k-1} + p^k \bar{A}_{k-1}, \qquad A' = A'_{k-1} + p^k \bar{A}'_{k-1},$$

so ist also die Bedingung der Kongruenz modulo p^k gegeben durch:

$$A_{k-1} = A'_{k-1},$$

und hieraus folgt sofort, daß $A - A' = p^k(\bar{A}_{k-1} - \bar{A}'_{k-1})$ ist, d. h. der Satz:

> Zwei Zahlen sind dann und nur dann modulo p^k kongruent, wenn ihre Differenz durch p^k teilbar ist.

Bisher haben wir bei der Darstellung

$$A = a_0 + a_1 p + a_2 p^2 + \cdots + a_\varrho p^\varrho \tag{2}$$

einer Zahl für den Bereich von p vorausgesetzt, daß ihre Ziffern der Reihe $0, 1, \cdots p-1$ angehören, d. h. modulo p reduzierte ganze positive Zahlen sein sollen. Mitunter werden wir uns von dieser Beschränkung freimachen und auch Darstellungen:

(2a) $$A = \bar{a}_0 + \bar{a}_1 p + \bar{a}_2 p^2 + \cdots + \bar{a}_\sigma p^\sigma$$

zulassen, bei denen die Ziffern $\bar{a}_i$ beliebige ganze positive Zahlen sein können. Wir werden aber solche allgemeinere „nicht reduzierte" Darstellungen von der eindeutig bestimmten „reduzierten" Darstellung (1) genau unterscheiden. Es ist sehr leicht, eine solche nicht reduzierte Darstellung (2a) von A in die reduzierte Form (2) überzuführen. Zu diesem Zwecke forme ich (2a) identisch um, indem ich schreibe:

$$A = (\bar{a}_0 - p\varepsilon_1) + (\bar{a}_1 + \varepsilon_1 - p\varepsilon_2)\,p + (\bar{a}_2 + \varepsilon_2 - p\varepsilon_3)\,p^2 + \cdots$$
$$= a_0 + a_1 p + a_2 p^2 + \cdots.$$

Hier lassen sich nun die Zahlen $\varepsilon_1, \varepsilon_2, \varepsilon_3 \ldots$ auf eine einzige Weise so bestimmen, daß die neuen Koeffizienten $a_0, a_1, a_2, \ldots$ reduziert sind. Man erhält nämlich die folgenden linearen Bestimmungsgleichungen:

$$\bar{a}_0 = a_0 + p\varepsilon_1,$$
$$\varepsilon_1 + \bar{a}_1 = a_1 + p\varepsilon_2,$$
$$\varepsilon_2 + \bar{a}_2 = a_2 + p\varepsilon_3,$$
$$\cdots\cdots\cdots$$

Aus der ersten Gleichung bestimmt sich a_0 eindeutig als der kleinste positive Divisionsrest von $\bar{a}_0$ durch p, und ε_1 als der Quotient dieser Division ist ebenfalls eindeutig bestimmt; aus der zweiten Gleichung bestimmen sich ebenso a_1 und ε_2, usw. Diese Gleichungen ergeben also stets eine eindeutig bestimmte Lösung, wie groß auch ihre Zahl sein mag. Multiplizieren wir die Gleichungen des obigen Systems bzw. mit $1, p, p^2 \ldots$ und addieren sie, so heben sich die mit den Zahlen ε_i multiplizierten Glieder auf beiden Seiten fort, und wir erhalten genau die gesuchte reduzierte Darstellung.

Schreibt man auch die nicht reduzierte Darstellung (2a) in der abgekürzten Form:

$$A = \bar{a}_0, \bar{a}_1 \bar{a}_2 \cdots \bar{a}_\sigma,$$

so wird diese dadurch in die reduzierte Form übergeführt, daß man von links nach rechts gehend jede Ziffer $\bar{a}_i$ durch ihren kleinsten positiven Rest modulo p ersetzt, dafür aber die nach rechts benachbarte Ziffer $\bar{a}_{i+1}$ um ε_i vermehrt, wenn in der vorigen $\varepsilon_i p$ weggelassen wurde. Ist z. B.

$$A = 7{,}53086 \quad (3),$$

so erhält man durch sukzessive Transformation nach dem soeben angegebenen Verfahren die reduzierte Form von A folgendermaßen:

$$A = 7{,}53086 = 1{,}73086 = 1{,}15086 = 1{,}12186 = 1{,}12128$$
$$= 1{,}121222 \qquad (3).$$

Bei dieser nicht reduzierten, und falls p größer als 10 ist, auch bei der reduzierten Darstellung, können auch Zahlen als Koeffizienten der Potenzen von p auftreten, für die wir keine einfachen Zeichen mehr haben, wie 10, 11, ... In diesem Fall trennen wir die Koeffizienten der verschiedenen Potenzen bei der abgekürzten Darstellung durch einen etwas größeren Zwischenraum, so daß auch hier Mißverständnisse ausgeschlossen sind, z. B.:

$$A = 2,\ 13\ \ 15\ \ 7\ \ 2\ \ 3\ \ 8\ \ 16 \qquad (5).$$

Auch hier läßt sich die Überführung von A in die reduzierte Form ebenso leicht bewerkstelligen, wie vorher.

Schon oben haben wir gesehen, daß eine Zahl ungeändert bleibt, wenn man zwei aufeinanderfolgende Ziffern (a_i, a_{i+1}) durch

$$(a_i + p,\ \ a_{i+1} - 1)$$

ersetzt. Man kann also auch hier wie bei der gewöhnlichen Darstellung der Zahlen eine Ziffer durch „Borgen" von der nächstbenachbarten vergrößern. Der einzige Unterschied ist, daß man hier nicht von der nach links, sondern von der nach rechts benachbarten borgt. So ist z. B.

$$1,3\,0\,0\,4\,1 = 1,3\,0\,5\,3\,1 = 1,3\,5\,4\,3\,1 \qquad (5).$$

Die beiden ersten elementaren Operationen, die Addition und Multiplikation sind in dem Gebiete der ganzen Zahlen unbeschränkt ausführbar. Sind

$$A = a_0 + a_1 p + a_2 p^2 + \cdots, \qquad B = b_0 + b_1 p + b_2 p^2 + \cdots$$

zwei ganze Zahlen, so kann ihre Summe und ihr Produkt, allerdings nicht in der reduzierten Form, sofort hingeschrieben werden; es ist nämlich:

$$A+B = (a_0 + b_0) + (a_1 + b_1)\,p + (a_2 + b_2)\,p^2 + \cdots,$$
$$AB = a_0 b_0 + (a_0 b_1 + a_1 b_0)\,p + (a_0 b_2 + a_1 b_1 + a_2 b_0)\,p^2 + \cdots,$$

und diese Darstellungen sind dann nach der oben gegebenen Vorschrift in ihre reduzierte Form überzuführen. Tut man dies zunächst bei der Summe, so erkennt man leicht, daß zwei Zahlen in dieser Darstellung genau so addiert werden wie zwei Dezimalbrüche, nur beginnt die Addition nicht bei den letzten, sondern bei den ersten Ziffern a_0 und b_0; und falls eine der so sich ergebenden Ziffern größer als $(p-1)$ ausfällt, so wird nicht die nach links, sondern die nach rechts benachbarte Ziffer um die entsprechende Zahl von Einheiten vermehrt. Wörtlich dasselbe gilt auch für die Multiplikation für den Bereich von p. Man übersieht das Verfahren am einfachsten an den beiden folgenden Beispielen, in denen die Primzahl p gleich 5 angenommen ist:

$$\begin{array}{r} 2,\ 3\ 1\ 0\ 2\ 1\ 1\ 4 \\ +\ 3,\ 1_1\,4_1\,1_1\,2\ 0\ 2\ 1\ 3_1 \\ \hline 0,\ 0\ 1\ 2\ 4\ 1\ 3\ 0\ 4 \end{array} \quad (5)$$

Bei der Multiplikation erscheint das Verfahren am einfachsten, daß man zunächst alle Teilprodukte in der nicht reduzierten Form aufschreibt, diese addiert und dann erst am Schluß das Resultat auf die reduzierte Form bringt. Zur Erläuterung geben wir das Beispiel:

$$\begin{array}{lllllll} 1, & 3 & 2 & 4 & & & \\ 3, & 0 & 4 & 2 & & & \\ \hline 3, & 9 & 6 & 12 & & & \\ & & 4 & 12 & 8 & 16 & \\ & & & 2 & 6 & 4 & 8 \\ \hline 3, & 9 & 10 & 26 & 14 & 20 & 8 \\ =3, & 4 & 1 & 3 & 4 & 3 & 2\ 2. \end{array} \quad (5)$$

Es seien A und B zwei Zahlen und allgemein A_k und B_k für $k = 0, 1, 2 \cdots$ ihre Näherungswerte für den Bereich von p. Bezeichnet man nun mit $(A+B)_k$ und $(AB)_k$ die k^{ten} Näherungswerte der Summe und des Produktes von A und B, so bestehen für jede noch so hohe Potenz von p die Kongruenzen:

$$(A+B)_k \equiv A_k + B_k \pmod{p^{k+1}},$$
$$(AB)_k \equiv A_k B_k \pmod{p^{k+1}}.$$

Es gilt also der Satz:

Der k^{te} Näherungswert der Summe, bzw. des Produktes zweier Zahlen ist kongruent der Summe, bzw. dem Produkte der k^{ten} Näherungswerte dieser Zahlen für den Modul p^{k+1}.

Der Beweis ergibt sich sofort aus den Gleichungen:

$$A = A_k + p^{k+1}\bar{A}_k, \qquad B = B_k + p^{k+1}\bar{B}_k$$

durch Addition bzw. Multiplikation. Umgekehrt ist die Summe $A+B$ bzw. das Produkt AB zweier Zahlen A und B offenbar als diejenige Zahl eindeutig bestimmt, deren Näherungswerte für jede noch so hohe Potenz von p als Modul der Summe bzw. dem Produkt der entsprechenden Näherungswerte von A und B kongruent sind. Mit Hilfe dieser Definition können Summe und Produkt zweier Zahlen durch ihre Näherungswerte bis zu beliebig hoher Ordnung genau ebenso abgekürzt berechnet werden, wie dies beim Rechnen mit den gewöhnlichen Dezimalbrüchen der Fall ist. Wesentlich ist aber das theoretische Resultat, daß durch jene sukzessiven Kongruenzen $A+B$ und AB eindeutig bestimmt sind. Gerade diese Definition

werden wir auch bei den inversen Rechenoperationen, der Subtraktion und Division, benutzen, wenn der Bereich der ganzen positiven Zahlen zu klein ist, um die Resultate jener Operationen geschlossen darzustellen.

§ 4. Die Subtraktion. Erweiterung des Gebietes der ganzen Zahlen durch Einführung der Zahlen für den Bereich von p oder der allgemeinen p-adischen Zahlen.

Wir haben gesehen, daß die beiden ersten elementaren Operationen, die Addition und Multiplikation, in dem von uns bisher betrachteten Bereiche der ganzen positiven Zahlen unbeschränkt ausführbar sind. Dasselbe gilt nicht mehr für die beiden inversen Operationen, die Subtraktion und die Division, und das kann auch nicht der Fall sein; denn die erste dieser beiden Operationen ist nur dann unbeschränkt ausführbar, wenn man die negativen, die zweite nur, wenn man die gebrochenen Zahlen hinzunimmt. Diese beiden Klassen von Zahlgrößen sind Rechnungssymbole, deren Bezeichnung zunächst willkürlich ist. Nur muß die Einführung so geschehen, daß die fundamentalen Gesetze, die für das Rechnen mit den ganzen positiven Zahlen gelten, auch in dem erweiterten Gebiete erhalten bleiben. Wir wollen die negativen und gebrochenen Zahlen für den Bereich von p in einer neuen, für die hier auftretenden Fragen zweckmäßigeren Weise definieren, und die so sich ergebende Erweiterung des Zahlbegriffes wird ihre Brauchbarkeit bei allen tiefer gehenden Untersuchungen der Arithmetik bewähren.

Sind zwei ganze Zahlen gegeben:

$$A = a_0, a_1 a_2 \cdots a_\varrho, \qquad B = b_0, b_1 b_2 \cdots b_\varrho \qquad (p),$$

die von gleicher Ziffernzahl vorausgesetzt werden können, da jeder Zahl rechts beliebig viele Nullen zugefügt werden dürfen, so versteht man unter ihrer Differenz $A - B$ eine Zahlgröße

$$C = c_0, c_1 c_2 \cdots \qquad (p),$$

welche der Gleichung

$$(1) \qquad B + C = A \qquad (p)$$

oder der Bedingung

$$(1\text{a}) \quad (b_0 + c_0) + (b_1 + c_1)\,p + (b_2 + c_2)\,p^2 + \cdots = a_0 + a_1 p + a_2 p^2 + \cdots$$

genügt. Ich muß also die noch unbekannten Größen $c_0, c_1, c_2 \ldots$ als Zahlen der Reihe $0, 1, \cdots p-1$ so bestimmen, daß die auf der linken Seite von (1a) stehende Zahl, nachdem sie auf die reduzierte Form gebracht ist, mit der Zahl A übereinstimmt. Zu diesem Zwecke schreibe ich $B + C$ in der Form:

$$(b_0 + c_0) + (b_1 + c_1)p + (b_2 + c_2)p^2 + \cdots$$
$$= (b_0 + c_0 - p\varepsilon_1) + (\varepsilon_1 + b_1 + c_1 - p\varepsilon_2)p + (\varepsilon_2 + b_2 + c_2 - p\varepsilon_3)p^2 + \cdots,$$

wo die $\varepsilon_1, \varepsilon_2, \varepsilon_3 \ldots$ so zu bestimmen sind, daß die betreffenden Koeffizienten bzw. gleich $a_0, a_1, a_2 \ldots$ werden. Es ergeben sich also für die $c_0, c_1, c_2 \ldots$ folgende Bestimmungsgleichungen:

$$\begin{aligned} b_0 + c_0 - p\varepsilon_1 &= a_0, \\ \varepsilon_1 + b_1 + c_1 - p\varepsilon_2 &= a_1, \\ \varepsilon_2 + b_2 + c_2 - p\varepsilon_3 &= a_2, \\ \vdots \qquad\qquad & \quad \vdots \end{aligned} \tag{2}$$

oder, wenn wir sie nach den Koeffizienten c_i auflösen:

$$\begin{aligned} c_0 &= a_0 - b_0 + p\varepsilon_1, \\ c_1 &= a_1 - b_1 + p\varepsilon_2 - \varepsilon_1, \\ c_2 &= a_2 - b_2 + p\varepsilon_3 - \varepsilon_2, \\ \vdots & \qquad\quad \vdots \\ c_{i-1} &= a_{i-1} - b_{i-1} + p\varepsilon_i - \varepsilon_{i-1}, \\ \ldots & \ldots\ldots\ldots\ldots \end{aligned} \tag{2a}$$

Hieraus bestimmen sich nacheinander die $c_0, c_1, c_2 \ldots$ eindeutig als reduzierte Zahlen; die $\varepsilon_1, \varepsilon_2, \varepsilon_3 \ldots$ bestimmen sich gleichfalls eindeutig, und zwar ist ε_i gleich 0 oder 1, je nachdem a_{i-1} nicht kleiner oder kleiner als $(b_{i-1} + \varepsilon_{i-1})$ ist.

Die so sich ergebende Vorschrift für die Subtraktion einer Zahl $B = b_0, b_1 b_2 \cdots b_\varrho$ von einer andern $A = a_0, a_1 a_2 \cdots a_\varrho$ stimmt also vollständig mit derjenigen für die Subtraktion eines Dezimalbruches von einem andern überein. Nur muß man auch hier wieder die Operation mit den beiden ersten Ziffern links, d. h. mit a_0 und b_0 beginnen und sich, falls $b_0 > a_0$ ist, eine Einheit der folgenden Stelle borgen usw. Zum Zeichen, daß ich von einer Stelle eine Einheit geborgt habe, setze ich einen Punkt vor die betreffende Zahl. Zur Veranschaulichung führe ich das folgende Beispiel durch, bei dem $p = 5$ gewählt ist:

$$\begin{array}{r} 3',\ .1\ .3\ .0\ .0\ .2\ .3\ .1 \\ -\ \underline{4,\ \ 2\ \ 4\ \ 3\ \ 2\ \ 3\ \ 4\ \ 0} \\ 4,\ \ 3\ \ 3\ \ 1\ \ 2\ \ 3\ \ 3\ \ . \end{array} \tag{5}$$

Wählt man p größer, etwa gleich 17, so können wieder zweistellige Zahlen als Ziffern in unserer Darstellung auftreten. Doch das macht auch hier keinen Unterschied, sobald wir dies durch die Schreibweise deutlich machen, z. B.:

$$\begin{array}{r} 15,.12\ .3\ .11\ 12 \\ -\ 16,\ 13\ 12\ \ 0\ \ 8 \\ \hline 16,\ 15\ \ 7\ 10\ \ 4. \end{array} \quad (17)$$

Die Subtraktion ist immer ausführbar und ergibt stets ein eindeutig bestimmtes Resultat, wenn der Minuendus A im gewöhnlichen Sinne des Wortes größer als der Subtrahendus B oder diesem wenigstens gleich ist. Ist dagegen A kleiner als B, so können wir das Resultat der Subtraktion in dem bisherigen Gebiete der positiven ganzen Zahlen nicht darstellen, sondern müssen dies erst so erweitern, daß das Resultat der Operation $A - B$ einen Sinn erhält. Gewöhnlich geschieht das in der Weise, daß man jeder ganzen positiven Zahl B ein Symbol $B' = -B$ zuordnet, welches durch die Gleichung:

$$B + B' = 0$$

definiert ist, und dann nachweist, daß in dem so erweiterten Gebiete jede Operation $A - B$ ausführbar ist, da sie zu einer eindeutig bestimmten Zahlgröße dieses Bereiches führt.

Auch ich will das Gebiet der ganzen positiven Zahlen zunächst so erweitern, daß jede Subtraktion ausführbar ist. Sind

$$A = a_0, a_1 a_2 \cdots a_\varrho, \qquad B = b_0, b_1 b_2 \cdots b_\varrho$$

ganz beliebig gegeben und behält man sich bei beiden Zahlen vor, die auf die ϱ^{ten} Ziffern folgenden Stellen durch Nullen beliebig weit auszufüllen, so liefert uns die Auflösung der linearen Gleichungen (2a) eine eindeutig bestimmte, beliebig weit fortsetzbare Reihe modulo p reduzierter ganzer Zahlen:

(3) $$c_0, c_1, c_2, \cdots$$

welche aber, falls $A < B$ ist, nicht abbricht, wie ja auch die Darstellung rationaler Brüche in Form von Dezimalbrüchen in den meisten Fällen zu unendlichen Reihen führt. So ist z. B. der rationale Bruch $^1/_3$ dargestellt durch den nicht abbrechenden Dezimalbruch: $0,333\ldots$ Breche ich die Reihe (3) bei einem gewissen Gliede, etwa bei c_σ ab, betrachte ich also nur die aus den $(\sigma + 1)$ ersten Ziffern gebildete ganze Zahl:

$$C_\sigma = c_0 + c_1 p + c_2 p^2 + \cdots + c_\sigma p^\sigma,$$

so genügt diese Zahl allerdings nicht der Gleichung:

$$A - B = C_\sigma,$$

stellt also die Differenz $A - B$ nicht genau dar; wohl aber genügt die ganze Zahl C_σ der Kongruenz:

(4) $$A_\sigma - B_\sigma \equiv C_\sigma \pmod{p^{\sigma+1}}$$

für jeden noch so großen Wert von σ. Multipliziert man nämlich die Gleichungen (2a) der Reihe nach mit $1, p, p^2 \ldots p^\sigma$, addiert sie und läßt die sich forthebenden Glieder $p^i \varepsilon_i$ fort, so erhält man:

$$C_\sigma = A_\sigma - B_\sigma + p^{\sigma+1} \varepsilon_{\sigma+1}; \tag{4a}$$

die Differenz von $(A_\sigma - B_\sigma)$ und C_σ ist also in der Tat durch $p^{\sigma+1}$ teilbar. Ist $\sigma > \varrho$, so sind alle Näherungswerte A_σ und B_σ gleich A bzw. gleich B, und die Kongruenz (4) geht dann für jede noch so hohe Potenz von p über in:

$$C_\sigma \equiv A - B \pmod{p^{\sigma+1}}. \tag{4b}$$

Wir wollen nun im folgenden die a. S. 7 gegebene Definition der Näherungswerte in der Weise erweitern, daß wir die eindeutig bestimmte Folge der positiven ganzen Zahlen:

$$C_0 = c_0 \quad C_1 = c_0, c_1 \quad C_2 = c_0, c_1 c_2 \cdots \quad C_\sigma = c_0, c_1 \cdots c_\sigma, \cdots$$

als den nullten, ersten, zweiten ... Näherungswert einer neuen noch unbekannten Zahlgröße C definieren. Dann folgt aus (4b) daß jene Näherungswerte C_σ zwar nicht gleich $A - B$, wohl aber bei genügend großem σ in bezug auf jede noch so hohe Potenz von p kongruent $A - B$ sind.

Die hier eingeführten neuen Zahlgrößen C sind den Irrationalzahlen in der elementaren Arithmetik sehr ähnlich. So können wir dort z. B. die Zahl π nicht genau durch einen Dezimalbruch darstellen; dagegen kennen wir ein Verfahren, das uns ermöglicht, die sämtlichen Näherungswerte von π auf eindeutige Weise zu bestimmen und damit π beliebig genau zu berechnen. Auf Grund dieser Eigenschaft sehen wir die Zahl π als bestimmt an und definieren sie als den Grenzwert ihrer Näherungswerte.

Es liegt daher nahe, auch hier den Begriff der Zahl auf die unendliche Reihe wohldefinierter Ziffern:

$$C = c_0, c_1 c_2 \cdots \qquad (p)$$

auszudehnen und die Differenz $A - B$ auch in dem Falle $A < B$ durch das Rechnungssymbol:

$$C = c_0, c_1 c_2 \cdots \qquad (p)$$

zu definieren, dessen Ziffern, so weit man will, aus den Gleichungen (2a) berechnet werden können. Dann ist der einzige Unterschied zwischen den beiden Fällen $A \geq B$ und $A < B$ der, daß im ersten von c_ϱ ab alle Ziffern Null sind, während sich im zweiten die Reihe der von Null verschiedenen Ziffern ins Unendliche erstreckt.

Schon diese erste Aufgabe führt uns also dazu, das Gebiet der positiven ganzen Zahlen durch die folgende Definition allgemeinerer Zahlgrößen zu erweitern:

Unter einer Zahlgröße für den Bereich von p oder einer p-adischen Zahl will ich jede Reihe:

$$c_0 + c_1 p + c_2 p^2 + c_3 p^3 + \cdots$$

mit modulo p reduzierten Koeffizienten, mag sie nun abbrechen oder nicht, verstehen, wenn eine Vorschrift existiert, nach welcher ihre Ziffern oder Koeffizienten soweit berechnet werden können als man nur immer will*).

In diesem erweiterten Bereich der p-adischen Zahlen führt jede Subtraktion zu einem eindeutig bestimmten Resultate; ich werde aber gleich zeigen, daß auch jeder Quotient $\frac{A}{B}$ gleich einer einzigen Zahlgröße dieses erweiterten Bereiches ist. Entschließt man sich nun, diesen Zahlgrößen von vornherein das gleiche Bürgerrecht mit den ganzen positiven Zahlen oder den abbrechenden Reihen zu geben, so lassen sich die tiefsten Fragen der Arithmetik höchst einfach beantworten, ebenso einfach wie die entsprechenden Fragen der Funktionentheorie.

*) Zu der gleichen Erweiterung unseres Bereiches werden wir auch durch die folgende Betrachtung geführt. Gehen wir von dem Grundelemente p aus, so ergibt sich aus ihm durch die elementaren Operationen der Multiplikation die beliebig weit zu verlängernde Reihe der Elemente:

$$1, p, p^2, \ldots$$

welche ineinander überführbar sind, da ja allgemein $p \cdot p^i = p^{i+1}$ ist.

Eine Zahlgröße C soll nun wohl definiert heißen, wenn wir von jedem Elemente p^i angeben können, wie oft es in C vorkommt. Kommt allgemein das Element p^i c_i Male in C vor, so soll C durch die Reihe

$$C = c_0 + c_1 p + c_2 p^2 + \cdots + c_i p^i + \cdots$$

definiert werden. Enthält C von einem Element p^n an kein einziges von den folgenden, so ist C eine positive ganze Zahl; ist dies nicht der Fall, so gehört eben C dem erweiterten Zahlgebiete an, dessen Eigenschaften im folgenden Kapitel genauer untersucht werden sollen.

Zweites Kapitel.

Die Zahlen des Körpers $K(p)$ und die elementaren Rechenoperationen.

§ 1. Die allgemeinen p-adischen Zahlen. Ihre Größe. Die Näherungswerte dieser Zahlen. Reduzierte und nicht reduzierte p-adische Zahlen. Definition der Gleichheit für reduzierte und nicht reduzierte Zahlen.

Wir hatten gesehen, daß die Forderung, die Subtraktion unbeschränkt auszuführen, notwendig zur Erweiterung des Zahlgebietes für den Bereich von p führt, indem jetzt jede begrenzte oder unbegrenzte Reihe mit ganzzahligen, modulo p reduzierten Koeffizienten:

$$(1) \qquad C = c_0 + c_1 p + c_2 p^2 + \cdots + c_k p^k + \cdots = \sum_0^{\infty} c_i p^i$$

als Zahlgröße für den Bereich von p oder als p-adische Zahl definiert wird, falls eine Vorschrift gegeben ist, ihre Koeffizienten soweit zu berechnen, als man nur immer will. Auch eine solche Zahl wollen wir abgekürzt in der Form

$$(1\text{a}) \qquad C = c_0, c_1 c_2 \cdots c_k \cdots$$

schreiben, welche sich von der a. S. 7 gegebenen nur dadurch unterscheidet, daß hier die Reihe der Ziffern $c_0, c_1, c_2, \ldots$ im allgemeinen nicht abbricht. Eine solche Zahl (1a) soll nur als ein Symbol, als eine Zusammenfassung der unendlich vielen gesetzmäßig gebildeten Ziffern $c_0, c_1, c_2, \ldots$ aufgefaßt werden, mit dem nach bestimmten gleich anzugebenden einfachen Gesetzen gerechnet wird; bricht die Reihe der Ziffern ab, so stellt die p-adische Zahl C eine eindeutig bestimmte positive ganze Zahl dar.

Das einzige Bedenken, das gegen diese Erweiterung des Bürgerrechtes für die Zahlen geltend gemacht werden könnte, ist das, daß eine solche unbegrenzte Reihe, wenn man sie in gewöhnlicher Weise summieren würde, eine unendliche Summe ergäbe. Aber das tritt

eben nur dann ein, wenn wir an der gewöhnlichen Definition der Größe festhalten; wir sind jedoch heutigentags weit von dem Standpunkte entfernt, das Maß oder die Größe einer Zahl oder einer geometrischen Figur als etwas von Natur und mit Notwendigkeit Gegebenes anzusehen. Wir betrachten die Größe einer Figur oder einer Zahl vielmehr als eine Funktion ihrer Bestimmungsstücke, deren Festsetzung ganz in unser Belieben gestellt ist, und bei deren Wahl wir uns nur durch Gründe der Zweckmäßigkeit leiten lassen. So definiert man z. B. als Größe oder als den absoluten Betrag einer komplexen Zahl $x+yi$ den Ausdruck $+\sqrt{x^2+y^2}$. Ein innerer, der Natur des Größenbegriffes entnommener Grund dafür liegt nicht vor und von vornherein könnte man ebenso gut daran denken, als Größe irgend einen anderen Ausdruck festzusetzen, etwa $\sqrt{\lambda x^2+\mu y^2}$, wo λ und μ positive Konstante sind. Die Rechtfertigung und Begründung der gewöhnlichen Definition der Größe einer komplexen Zahl liegt in ihrer Nützlichkeit für analytische Untersuchungen und vor allem auch in der einfachen und anschaulichen geometrischen Deutung, die ihr von Gauß gegeben wurde. Wir erinnern noch an die Größendefinitionen in den Nichteuklidischen Geometrieen, die von der gewöhnlichen Definition oft sehr verschieden sind und deren Wahl wiederum nur durch die mit ihrer Hilfe erreichte Einfachheit und Klarheit gerechtfertigt wird.

Um für die p-adischen Zahlen eine praktische Definition der Größe aufzufinden, orientieren wir die Betrachtung zunächst wieder an den entsprechenden Fragen der Funktionentheorie und stellen uns die Aufgabe, bei den durch Potenzreihen dargestellten Funktionen eine zweckmäßige Größendefinition zu geben. Es seien uns für die Umgebung einer Stelle $z=a$ zwei Funktionselemente

$$f(z)=a_\varrho(z-a)^\varrho+a_{\varrho+1}(z-a)^{\varrho+1}+\cdots,$$
$$g(z)=b_\sigma(z-a)^\sigma+b_{\sigma+1}(z-a)^{\sigma+1}+\cdots$$

gegeben, deren Ordnungszahlen für die Stelle $z=a$ bzw. ϱ und σ sind. Wenn man diese Funktionen in einer genügend kleinen Umgebung des Punktes $z=a$ betrachtet, so überwiegt das erste Glied an Größe die Summe aller anderen, und die Funktion ist um so größer, je größer das erste Glied für genügend kleine Werte von $(z-a)$ ist. Vergleicht man zwei Funktionen in bezug auf ihre Größe für die Stelle $z=a$, so erkennt man bei Bildung des Quotienten, daß diejenige die größere ist, deren Ordnungszahl kleiner ist. Auf diese Weise erhält man eine einwandfreie und zweckmäßige Größenordnung der Funktionen, wenn man noch zwei Funktionen gleich groß nennt, falls ihre Ordnungszahlen übereinstimmen. Diese Vergleichung gilt

jedoch nur für die Umgebung der Stelle $z = a$; denn bei dem Übergang zu einer anderen Stelle $z = b$ erhält man ja andere Ordnungszahlen von $f(x)$ und $g(x)$, und damit wird das Größenverhältnis dieser Funktionen an der Stelle $z = b$ ein anderes. Für jede einzelne Stelle erhält man also eine zweckmäßige Größenbestimmung, wenn man die negative Ordnungszahl als Maßzahl einführt.

Diesen selben Gedanken wollen wir festhalten für die Definition der Größe im Bereich der Primzahl p. Sind uns zwei p-adische Zahlen gegeben:

$$C = c_\varrho p^\varrho + c_{\varrho+1} p^{\varrho+1} + \cdots = 0, 0\,0 \cdots c_\varrho c_{\varrho+1} \cdots,$$
$$D = d_\sigma p^\sigma + d_{\sigma+1} p^{\sigma+1} + \cdots = 0, 0\,0 \cdots\cdots c_\sigma c_{\sigma+1} \cdots,$$

so wollen wir diejenige als die größere für den Bereich von p bezeichnen, deren Ordnungszahl die kleinere ist, während Zahlgrößen von gleicher Ordnungszahl als von gleicher Größe oder als äquivalent betrachtet werden. Von zwei p-adischen Zahlen C und D ist also diejenige die kleinere, welche mehr Nullen hinter dem Komma hat. C und D sind äquivalent, wenn beide gleich viele Nullen hinter dem Komma haben. An dieser Definition wollen wir vorläufig festhalten; erst später, wenn wir unsere Untersuchung von der Beschränkung auf den Bereich einer einzigen Primzahl frei machen, und dieselbe Zahlgröße C für den Bereich verschiedener Primzahlen p oder q usw. studieren, werden wir statt der Ordnungszahl ϱ ein Vielfaches $\varrho \cdot c$ derselben einführen, in welchem der Faktor c aber nur von p abhängt. Solange wir verschiedene Zahlen für den Bereich derselben Primzahl p untersuchen, ändert sich dieser Faktor c nicht und ist somit bedeutungslos; daher behalten alle über die Ordnungszahlen hier anzugebenden Resultate auch später ihre Gültigkeit. Es wird also jetzt jede unserer Zahlen, mag die Reihe ihrer Koeffizienten abbrechen, oder sich ins Unendliche fortsetzen, ihrer Größe nach durch eine ganze positive Zahl oder die Null charakterisiert, und gerade diese Definition wird sich für unsere späteren Zwecke als besonders praktisch erweisen.

Nachdem wir so die Bedenken gegen die Einführung der p-adischen Zahlen zurückgewiesen haben, wollen wir sofort von dem Bereich aller so definierten Zahlgrößen ausgehen, die elementaren Rechenoperationen nach einem allgemeinen Prinzipe definieren und dann zeigen, daß innerhalb des erweiterten Bereiches zunächst die vier elementaren Rechenoperationen unbeschränkt ausführbar sind.

Es sei

$$A = a_0 + a_1 p + a_2 p^2 + \cdots = a_0, a_1 a_2 \cdots \qquad (p)$$

eine p-adische Zahl; dann führen wir auch hier den Begriff ihrer Näherungswerte ein. Die ganzen, aus A durch Fortlassung der späteren Ziffern hervorgehenden positiven ganzen Zahlen

$$A_0 = a_0, \quad A_1 = a_0, a_1 = a_0 + a_1 p, \quad A_2 = a_0, a_1 a_2 = a_0 + a_1 p + a_2 p^2, \cdots$$

sollen wieder der nullte, erste, zweite, ... Näherungswert von A für den Bereich von p heißen. Diese Näherungswerte bilden eine wohldefinierte Reihe ganzer positiver Zahlen, für welche allgemein:

$$A_k = A_{k-1} + a_k p^k,$$

also

$$A_k \equiv A_{k-1} \pmod{p^k}$$

ist. Der einzige Unterschied gegen den a. S. 8 betrachteten einfacheren Fall der ganzen positiven Zahlen ist der, daß hier in der unendlichen Reihe

$$A_0, \; A_1, \; A_2, \; \ldots$$

der Näherungswerte von A diese ganzen Zahlen im allgemeinen nicht von einer bestimmten an alle denselben Wert haben, genau ebenso wie dies bei den gewöhnlichen irrationalen Zahlen, z. B. bei den Näherungswerten $3 \quad 3,1 \quad 3,14 \quad 3,141 \; \ldots$ der Zahl π der Fall ist.

Zwei p-adische Zahlen

$$A = a_0, a_1 a_2 a_3 \cdots, \qquad A' = a_0', a_1' a_2' a_3' \cdots \qquad (p)$$

heißen wieder kongruent für den Modul p^{k+1}, wenn ihre k^{ten} Näherungswerte A_k und A_k' noch übereinstimmen, oder was dasselbe ist, wenn ihre $(k+1)$ ersten Ziffern $a_0, a_1, \ldots a_k$ und $a_0', a_1' \cdots a_k'$ bezüglich gleich sind.

Zwei Zahlgrößen A und A' unseres Bereiches sollen ferner gleich heißen, wenn sie für jede noch so hohe Potenz von p als Modul einander kongruent sind. Sind dann zwei solche Größen einer und derselben dritten gleich, so sind sie untereinander gleich. Zwei Zahlen A und A' sind dann und nur dann einander gleich, wenn für jeden noch so großen Wert von k immer $a_k = a_k'$ ist, wenn also je zwei entsprechende Ziffern gleich sind. Wären nämlich a_k und a_k' die ersten von einander verschiedenen Ziffern, so wären zwar $A_0 = A_0', \cdots A_{k-1} = A_{k-1}'$, aber $A_k \gtrless A_k'$, und es ist daher schon die Kongruenz

$$A \equiv A' \pmod{p^{k+1}}$$

nicht erfüllt und dasselbe gilt a fortiori für jede höhere Potenz von p als Modul.

Durch ihre Näherungswerte ist eine p-adische Zahl A mit jeder beliebigen Genauigkeit bestimmt; denn die Differenz $A - A_k$ ist durch p^{k+1} teilbar und wird daher nach unserer Definition der Größe um so

kleiner, je größer ich k wähle. Da wir eine Größe, deren Ordnungszahl unendlich groß ist, als unendlich klein bezeichnen müssen, so verfahren wir konsequent, wenn wir die Zahl A als den Grenzwert ihrer Näherungswerte definieren, also setzen:

$$A = \lim_{k=\infty} A_k \quad (p).$$

Denn mit dieser Definition tragen wir gerade dem oben eingeführten Begriff der Gleichheit Rechnung. Wir können diesem Grenzprozeß auch noch andere Formen geben, indem wir z. B.

$$A = A_0 + (A_1 - A_0) + (A_2 - A_1) + \cdots + (A_k - A_{k-1}) + \cdots \quad (p)$$

schreiben. Brechen wir diese Reihe mit dem $(k+1)^{\text{ten}}$ Gliede ab, so bleibt genau A_k übrig, diese Reihe stellt also wirklich die Zahl A dar.

Sind in der Entwicklung von A die ersten α Koeffizienten gleich Null, ist also

$$A = a_\alpha p^\alpha + a_{\alpha+1} p^{\alpha+1} + \cdots,$$

so sage ich, A besitzt für den Bereich von p die Ordnungszahl α.

Eine Zahl E, deren Ordnungszahl Null ist, in deren Entwicklung:

$$E = e_0 + e_1 p + e_2 p^2 + \cdots,$$

also der erste Koeffizient e_0 nicht Null ist, heißt wieder eine Einheit für den Bereich von p.

Wir wollen auch hier von der Beschränkung absehen, daß die Koeffizienten $a_0, a_1, a_2, \ldots$ modulo p reduzierte Zahlen sein sollen und auch solche Reihen:

$$\bar{A} = \bar{a}_0 + \bar{a}_1 p + \bar{a}_2 p^2 + \cdots$$

als p-adische Zahlen bezeichnen, in denen die Koeffizienten $\bar{a}$ nicht modulo p reduzierte, sondern beliebige ganze positive Zahlen sind.

Die ganzen positiven Zahlen:

$$\bar{A}_0 = \bar{a}_0, \quad \bar{A}_1 = \bar{a}_0, \bar{a}_1, \quad \bar{A}_2 = \bar{a}_0, \bar{a}_1 \bar{a}_2, \cdots$$

sollen wieder der nullte, erste, zweite, ... Näherungswert von $\bar{A}$ für den Bereich von p heißen. Diese Näherungswerte sind wohldefiniert und eindeutig bestimmt für eine jede nicht reduzierte Darstellung. Es besteht für sie ebenfalls die Gleichung:

$$\bar{A}_k = \bar{A}_{k-1} + \bar{a}_k p^k,$$

oder die damit gleichwertige Kongruenz:

$$\bar{A}_k \equiv \bar{A}_{k-1} \pmod{p^k}.$$

Auch die Zahl $\bar{A}$ ist durch die Reihe ihrer Näherungswerte mit jeder vorgegebenen Genauigkeit bestimmt, und wir können sie deshalb definieren durch die Gleichung:

$$\bar{A} = \lim_{k=\infty} \bar{A}_k \quad (p).$$

Zwei reduzierte oder nicht reduzierte Zahlen heißen **kongruent für den Modul** p^{k+1}, wenn ihre k^{ten} Näherungswerte für diesen Modul kongruent sind; sie heißen **gleich für den Bereich von** p, wenn sie für jede noch so hohe Potenz von p als Modul kongruent sind. Sind zwei solche Zahlen einer dritten gleich, so sind sie einander gleich.

Man sieht leicht, daß alle bisher ausgesprochenen Sätze und Definitionen im allgemeinen auch für die nicht reduzierten Darstellungen gültig bleiben. Doch das Rechnen mit den nicht reduzierten Zahlen gewinnt seine sichere Grundlage erst durch den folgenden Satz:

Jede nicht reduzierte p-adische Zahl

$$\bar{A} = \bar{a}_0, \bar{a}_1 \bar{a}_2 \cdots \quad (p)$$

ist einer und nur einer reduzierten Zahl:

$$A = a_0, a_1 a_2 \cdots \quad (p)$$

gleich.

Daß es **eine** solche reduzierte Zahl gibt, der $\bar{A}$ gleich ist, zeigen wir durch das folgende Verfahren: Man bestimme in den sukzessiven Gleichungen:

$$(2) \qquad \begin{aligned} \bar{a}_0 &= a_0 + p\varepsilon_1, \\ \varepsilon_1 + \bar{a}_1 &= a_1 + p\varepsilon_2, \\ &\vdots \\ \varepsilon_k + \bar{a}_k &= a_k + p\varepsilon_{k+1} \\ &\vdots \end{aligned}$$

die Größen $a_0, a_1 \ldots a_k \ldots$ als Zahlen der Reihe $0, 1 \cdots p-1$. Damit sind sie eindeutig definiert, und auch die ε ergeben sich als eindeutig bestimmte Zahlen. Multipliziert man diese Gleichungen bzw. mit $1, p, \ldots p^k \ldots$ und addiert sie, so heben sich, wenn wir bis zur $(k+1)^{\text{ten}}$ Gleichung gehen, auf beiden Seiten die Glieder mit ε weg mit Ausnahme des Gliedes $p^{k+1}\varepsilon_{k+1}$, und wir erhalten die Gleichung:

$$\bar{a}_0 + \bar{a}_1 p + \cdots + \bar{a}_k p^k = a_0 + a_1 p + \cdots + a_k p^k + \varepsilon_{k+1} p^{k+1},$$

und damit die gesuchte Darstellung, da wir das k beliebig groß wählen können. Diese Zahl $a_0, a_1 a_2 \ldots$ ist auch eindeutig bestimmt; denn wäre dieselbe Zahl $\bar{A}$ zwei reduzierten Zahlen gleich, so müßten diese untereinander gleich sein und dies ist nur möglich, wenn alle ihre Ziffern bzw. übereinstimmen, wenn sie also identisch sind. Hieraus folgt noch sofort der Satz:

Zwei nicht reduzierte Zahlen sind dann und nur dann gleich, wenn die zugehörigen reduzierten Zahlen identisch sind. Die praktische Methode, eine Zahl $\bar{A}$ auf ihre reduzierte Form zu bringen ist genau die a. S. 9 für abbrechende Reihen gegebene, nur ist hier eben die bei a_0 beginnende und von links nach rechts gehende Umformung so weit fortzusetzen, als es der Zweck der jedesmaligen Untersuchung erfordert. So ergibt z. B. eine leichte Rechnung die Richtigkeit der folgenden Gleichung:

$$1,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12 \cdots = 1,2\,0\,2\,0\,2\,0\,2\,0\,2\,0\,2\,0 \cdots \qquad (3).$$

Als zweites besonders wichtiges Beispiel führe ich die Darstellung der Null für den Bereich von p an. Es ist nämlich die Zahl

$$O = p,\,(p-1)\,(p-1)\,(p-1)\cdots \qquad (p)$$

gleich Null, da sie gleich der Reihe:

$$O = p + p(p-1) + p^2(p-1) + \cdots$$

ist, deren Näherungswerte $O_k = p^{k+1}$ mit wachsendem k durch jede noch so hohe Potenz von p teilbar, also denen der reduzierten Zahl $0 = 0,0\,0\,0\cdots$ kongruent sind. Man sieht an diesem Beispiel, daß man sich bei einer nicht reduzierten Zahl nicht durch die Größe der Koeffizienten täuschen lassen darf; man muß sie vielmehr zunächst auf die reduzierte Form bringen, ehe man sie hinsichtlich ihrer Größe untersucht. Ebenso ist die Reihe:

$$O = 0,0\,0\cdots 0\,p\,(p-1)\cdots = p^r\cdot p + p^{r+1}(p-1) + \cdots$$

gleich Null, da ihre Näherungswerte $O_{r+k} = p^{r+k}$ sind, also mit denen der vorigen Reihe übereinstimmen. Allgemein stellt eine Zahl

$$O = o_0,\,o_1\,o_2\,o_3\cdots \qquad (p)$$

dann und nur dann die Null dar, wenn die zugehörige reduzierte Zahl lauter verschwindende Koeffizienten hat, d. h. wenn für alle Indizes k die Gleichungen bestehen:

$$\begin{aligned} o_0 &= p\,\varepsilon_1, \\ \varepsilon_1 + o_1 &= p\,\varepsilon_2, \\ &\vdots \\ \varepsilon_{k-1} + o_{k-1} &= p\,\varepsilon^k, \\ &\cdots\cdots \end{aligned}$$

So ist z. B. die Zahl

$$O = p,\,(2p-1)\,(3p-2)\,(4p-3)\,(5p-4)\cdots \qquad (p)$$

gleich Null, und dasselbe gilt für die Zahl:

$$p^2,\,(2p^2-2p)\,\,(3p^2-4p+1)\,\,(4p^2-6p+2)\,\,(5p^2-8p+3)\cdots,$$

wie sich nach einer leichten Rechnung ergibt.

Endlich erweitere ich den Begriff der nicht reduzierten p-adischen Zahlen dadurch, daß ich auch solche Reihen

(3) $$\bar{a}_0 + \bar{a}_1 p + \cdots$$

als p-adische Zahlen zulasse, deren Koeffizienten $\bar{a}_i$ nur modulo p ganze Zahlen, nämlich solche positive oder negative rationale Brüche sind, deren Nenner in der reduzierten Form durch p nicht teilbar sind. Auch für sie gelten die vorher angegebenen Sätze, insbesondere das Hauptresultat, daß jede nicht reduzierte p-adische Zahl einer einzigen reduzierten gleich ist. Jede modulo p ganze Zahl $\bar{a} = \frac{a}{b}$ kann nämlich bekanntlich ebenfalls auf eine einzige Weise in der Form $\bar{a} = a + p\varepsilon$ geschrieben werden, wo a eine Zahl der Reihe $0\,1 \ldots p-1$ und $\varepsilon = \frac{a'}{b'}$ wieder eine modulo p ganze Zahl bedeutet. Also ist das Reduktionsverfahren (2) auch auf jede Reihe (3) anwendbar und ergibt eine eindeutig bestimmte reduzierte Zahl.

§ 2. Die Addition, Subtraktion und Multiplikation der p-adischen Zahlen. Folgerungen.

Auf Grund der a. S. 22 gegebenen Definition der Gleichheit zweier p-adischen Zahlen kann man nun leicht die Summe, die Differenz, das Produkt und den Quotienten solcher Zahlen definieren und zeigen, daß das Resultat einer jeden solchen Operation wieder eine eindeutig bestimmte p-adische Zahl ist.

Sind
$$A = a_0, a_1 a_2 \cdots, \qquad B = b_0, b_1 b_2 \cdots \quad (p)$$
zwei Zahlen unseres Bereiches, so ist nach unserer Definition der Gleichheit
$$C = A + B, \qquad D = A - B,$$
wenn für jede noch so hohe Potenz von p als Modul:

(1) $$C_i \equiv A_i + B_i, \qquad D_i \equiv A_i - B_i \pmod{p^{i+1}}$$

ist. Hiernach sind die Zahlen C und D zunächst in der nicht reduzierten Form durch die Gleichungen:

(2) $$\begin{aligned} C &= A + B = (a_0 + b_0) + p(a_1 + b_1) + \cdots, \\ D &= A - B = (a_0 - b_0) + p(a_1 - b_1) + \cdots \end{aligned}$$

eindeutig bestimmt, denn für sie sind ja die Kongruenzen (1) für jede noch so hohe Potenz p^k von p als Modul offenbar erfüllt. Diese Zahlen (2) kann man nach der a. S. 9 angegebenen Vorschrift dadurch auf ihre reduzierte Form bringen, daß man sie durch die ihnen gleichen Zahlen

(2a) $$\begin{aligned} C &= A + B = (a_0 + b_0 - p\varepsilon_1) + p(a_1 + \varepsilon_1 + b_1 - p\varepsilon_2) + \cdots, \\ D &= A - B = (a_0 - b_0 + p\varepsilon_1') + p(a_1 - \varepsilon_1' - b_1 + p\varepsilon_2') + \cdots \end{aligned}$$

ersetzt und die noch willkürlich bleibenden ganzen Zahlen ε_i und ε_i' so bestimmt, daß die dann sich ergebenden Koeffizienten von $1, p, p^2, \ldots$ modulo p reduzierte Zahlen werden, was sich immer auf eine einzige Weise erreichen läßt.

Die Definitionen der Summe und Differenz lassen sich auch durch die folgenden Gleichungen ausdrücken:

$$A \pm B = \lim_{k=\infty} (A_k \pm B_k), \tag{3}$$

welche deutlich erkennen lassen, daß man zur Bildung der Summe und Differenz zweier Zahlen nur die früheren Regeln für das Rechnen mit ganzen positiven Zahlen anzuwenden hat. Dies zeigt auch das folgende Beispiel:

$$\begin{array}{rl} & 2,\ \overline{1\,3\,1\,4}\,1\,3\,1\,4\ldots \\ + & 3,\ \overline{3\,1\,3\,0}\,3\,1\,3\,0\ldots \\ \hline & 0,\ 0\,0\,0\,0\,0\,0\,0\,0\ldots, \end{array} \qquad (5)$$

wo der Strich über den vier ersten Ziffern andeutet, daß beide Summanden je eine viergliedrige Periode haben. Die Summe der beiden Zahlen ist mithin gleich Null; wenn wir also die eine mit A, die andere mit A' bezeichnen, so besteht die Gleichung:

$$A + A' = 0 \qquad (5$$

d. h. es ist A' gleich $-A$.

Zur Erläuterung der Subtraktion diene das folgende Beispiel:

$$\begin{array}{rl} & 0,\ 0\,1\,2\,0\,1\,2\,0\,1\,2\,0\,1\,2\,0\,1\,2\ldots \\ - & 0,\ 2\,1\,0\,2\,2\,1\,0\,2\,2\,1\,0\,2\,2\,1\,0\ldots \\ \hline & 0,\ 1\,2\,1\,1\,1\,0\,0\,2\,2\,1\,0\,0\,1\,2\,1\ldots; \end{array} \qquad (3)$$

es werde beiläufig bemerkt, daß in diesem Falle auch die Differenz periodisch wird und ihre Periode $3 \cdot 4 = 12$ Ziffern enthält. Man kann die Subtraktion in dieser Weise nicht direkt ausführen, wenn der Minuendus eine geringere Anzahl Ziffern als der Subtrahendus besitzt. In diesem Falle hat man zu dem Minuendus die Zahl:

$$0, 0\,0 \ldots 0\ p\ (p-1)\ (p-1) \cdots \qquad (p)$$

zu addieren, die ja nach der Bemerkung a. S. 23 gleich Null ist, und zwar wählt man die Anzahl der Ziffern 0 von vornherein so, daß die Ziffer p gerade an die Stelle kommt, von welcher im Minuendus eine Einheit geborgt werden müßte, während dieser nur noch Nullen enthält. Auf diese Weise erhält man die späteren Ziffern ohne weitere Umformung sofort in der reduzierten Form. So ergibt sich z. B.:

$$\begin{array}{r} {\scriptstyle 5\;4\;4\,\ldots} \\ 2,3\,1.2.4.0.0.1\,0\,0\,0\,0\,0\,0\ldots \\ -\;1,2\,3\,4\,4\,4\,3\,0\,0\,0\,\bar{3}\,4\,3\,4\ldots \\ \hline 1,1\,3\,2\,4\,0\,1\,0\,0\,0\,2\,0\,\overline{1\,0}\,\overline{1\,0}\ldots. \end{array} \qquad (5)$$

Eine p-adische Zahl C ist gleich dem Produkte zweier anderer Zahlen A und B, wenn für jede noch so hohe Potenz von p als Modul

$$(4) \qquad C_k \equiv A_k B_k \pmod{p^{k+1}}$$

ist. Hieraus folgt sofort, daß es eine und nur eine Zahl C gibt, für welche die Gleichung

$$C = AB = (a_0 + a_1 p + a_2 p^2 + \cdots)(b_0 + b_1 p + b_2 p^2 + \cdots)$$

erfüllt ist, und daß dieses die Zahl:

$$(4a) \qquad C = a_0 b_0 + (a_0 b_1 + a_1 b_0) p + (a_0 b_2 + a_1 b_1 + a_2 b_0) p^2 + \cdots + (a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0) p^k + \cdots$$

ist, die dann nur noch auf ihre reduzierte Form gebracht werden muß. Bildet man nämlich die Näherungswerte:

$$C_k \quad \text{und} \quad A_k B_k$$

und läßt in dem Produkte rechts alle Potenzen von p fort, deren Exponenten größer als k sind, so ergibt sich in der Tat die obige Kongruenz (4) und damit der Beweis unseres Satzes. Auch die Definitionsgleichung des Produktes können wir mit Hilfe der Näherungswerte in der Form schreiben:

$$AB = \lim_{k=\infty} (A_k B_k) \qquad (p).$$

Es ist also auch die Multiplikation von zwei unbegrenzten Reihen A und B genau nach der a. S. 10 angegebenen Vorschrift für die Multiplikation von zwei ganzen Zahlen auszuführen; will man das Produkt C nur bis zum Näherungswerte C_k haben, so hat man die Multiplikation bei der k^{ten} Stelle abzubrechen, genau wie bei der abgekürzten Multiplikation der Dezimalbrüche. Hier ist die Rechnung aber noch einfacher, weil die Abschätzung der $(k+1)^{\text{ten}}$ Stelle unnötig ist. Das folgende Produkt wollen wir bis zur 10ten Stelle genau berechnen:

```
0,1 2 3 1 2 3 1 2 3 1 ...    (5)
0,0 0 2 1 2 1 2 1 2 1 ...
-------------------------
0,0 0 0 2 4 6 2 4 6 2
          1 2 3 1 2 3
            2 4 6 2 4
              1 2 3 1
                2 4 6
                  1 2
                    2
            1 2 2 3 4
-------------------------
0,0 0 0 2 0 1 2 2 1 4 ... .
```

Aus den bisher abgeleiteten Resultaten ziehen wir noch einige Folgerungen. Zunächst ist klar, daß für die von uns definierten elementaren Operationen das kommutative und assoziative Gesetz der Addition und Multiplikation, sowie das distributive Gesetz für die Verknüpfung der Addition und Multiplikation gelten, d. h. es bestehen die folgenden Gleichungen:

$$A + B = B + A, \qquad A + (B + C) = (A + B) + C,$$
$$AB = BA, \qquad A(BC) = (AB)C,$$
$$A(B + C) = AB + AC.$$

Ferner erkennt man unmittelbar, daß die drei Fundamentalsätze bestehen bleiben:

Gleiches zu Gleichem addiert gibt Gleiches.

Gleiches von Gleichem subtrahiert gibt Gleiches.

Gleiches mit Gleichem multipliziert gibt Gleiches.

Folgerung 1. Jede p-adische Zahl läßt sich auf eine einzige Weise in der Form

$$A = p^{\alpha} E$$

darstellen, wenn α die Ordnungszahl von A und E eine Einheit ist. Denn nach der Definition des Produktes ist ja:

$$A = a_{\alpha} p^{\alpha} + a_{\alpha+1} p^{\alpha+1} + \cdots = p^{\alpha}(a_{\alpha} + a_{\alpha+1} p^{\alpha+1} + \cdots),$$

wo der zweite Faktor wirklich eine Einheit ist. Auch hier soll die Potenz p^{α} der **absolute Betrag** von A genannt und durch $|A|$ bezeichnet werden.

Folgerung 2. Das Produkt zweier Einheiten ist wieder eine Einheit. Aus der Gleichung:

$$EE' = (e_0 + e_1 p + \cdots)(e_0' + e_1' p + \cdots) = e_0 e_0' + (e_0 e_1' + e_1 e_0') p + \cdots$$

folgt nämlich sofort, daß das Anfangsglied $e_0 e_0'$ von EE' nicht durch p teilbar sein kann, wenn für die Anfangsglieder von E und E' das Gleiche gilt.

Folgerung 3. Die Ordnungszahl eines Produktes ist stets gleich der Summe der Ordnungszahlen seiner Faktoren.

Ist nämlich

$$A = p^{\alpha} E, \qquad B = p^{\beta} E',$$

so ist in der Tat:

$$AB = p^{\alpha+\beta} EE' = p^{\alpha+\beta} \bar{E}$$

wo $\bar{E}$ wieder eine Einheit ist.

Folgerung 4. Das Produkt zweier oder mehrerer Zahlen ist dann und nur dann gleich Null, wenn mindestens einer der Faktoren Null ist.

Sind nämlich z. B. in dem Produkte AB beide Faktoren nicht Null, ist also $A = p^{\alpha} E$ und $B = p^{\beta} E'$, so ist ihr Produkt gleich $p^{\alpha+\beta} \bar{E}$, also sicher nicht gleich Null.

Folgerung 5. Jede Zahl unseres Bereiches kann als Summe einer positiven ganzen und einer für den Bereich von p beliebig kleinen Zahl dargestellt werden.

Ist nämlich A eine beliebige p-adische Zahl und A_k ihr k^{ter} Näherungswert, so ist für jeden noch so großen Wert von k:

$$\begin{aligned} A &= A_k + p^{k+1}(a_{k+1} + a_{k+2}p + \cdots) \\ &= A_k + \bar{A}_k \end{aligned}$$

und $\bar{A}_k$ ist mindestens von der Ordnung $(k+1)$, kann also in der Tat durch Vergrößerung von k beliebig klein gemacht werden.

Ist n eine beliebige zusammengesetzte ganze Zahl, so könnte man jede ganze positive Zahl A auch im n-adischen Zahlensysteme d. h. in der Form:

$$A = a_0 + a_1 n + a_2 n^2 + \cdots + a_k n^k = a_0, a_1 a_2 \cdots a_k \qquad (n)$$

darstellen und den Bereich alsdann durch Adjunktion der nicht abbrechenden n-adischen Zahlen

$$B = b_0 + b_1 n + \cdots + b_k n^k + \cdots = b_0, b_1 \cdots b_k \cdots \qquad (n)$$

erweitern. Würde man dann die Gleichheit zweier solchen Zahlen und auf dieser Grundlage die elementaren Rechenoperationen so definieren, daß sie für die abbrechenden Reihen gültig bleiben, so würde man ebenfalls zu einer vollkommen konsequenten Arithmetik gelangen, bei welcher aber der soeben als Folgerung 4 bewiesene Fundamentalsatz nicht richtig zu sein brauchte. So ist z. B. für die Grundzahl Zehn das Produkt der beiden Zahlen:

$$A = 5, 2\,1\,3\,0\,2\,3 \cdots \quad \text{und} \quad B = 2, 1\,1\,0\,1\,0\,0 \cdots$$

gleich Null, wie die folgende einfache Rechnung lehrt:

$$\begin{array}{r} 5,2\,1\,3\,0\,2\,3\ldots \\ 2,1\,1\,0\,1\,0\,0\ldots \\ \hline 10,4\,2\,6\,0\,4\,6\ldots \\ 5\,2\,1\,3\,0\,2\ldots \\ 5\,2\,1\,3\,0\ldots \\ 5\,2\,1\ldots \\ \hline 0,0\,0\,0\,0\,0\,0\ldots. \end{array}$$

Der Grund dieser merkwürdigen Tatsache ist der: Von den beiden Zahlen:

$$A = 5,2\,1\,3\,0\,2\,3\cdots = 5 + 2\cdot 10 + 1\cdot 10^2 + \cdots,$$
$$B = 2,1\,1\,0\,1\,0\,0\cdots = 2 + 1\cdot 10 + 1\cdot 10^2 + \cdots$$

ist die erste, als nicht reduzierte pentadische Zahl betrachtet, gleich Null, die zweite ist ebenfalls Null, wenn man sie als nicht reduzierte dyadische Zahl schreibt; dies ergibt sich unmittelbar aus der Darstellung:

$$(5)\quad \begin{aligned} A &= 5 + (2\cdot 2)\cdot 5 + (1\cdot 2^2)\cdot 5^2 + (3\cdot 2^3)\cdot 5^3 + (0\cdot 2^4)\cdot 5^4 + (2\cdot 2^5)\cdot 5^5 + \cdots, \\ B &= 2 + (1\cdot 5)\cdot 2 + (1\cdot 5^2)\cdot 2^2 + (0\cdot 5^3)\cdot 2^3 + (1\cdot 5^4)\cdot 2^4 + (0\cdot 5^5)\cdot 2^5 + \cdots. \end{aligned}$$

Also ist das Produkt AB nach dem soeben bewiesenen Satze für den Bereich der beiden Zahlen 2 und 5 gleich Null, und hieraus folgt leicht, daß dasselbe auch für den Bereich von 10 der Fall ist*).

Da nun der in der vierten Folgerung für die p-adischen Zahlen bewiesene Satz das Fundament der gesamten Arithmetik ist, so würde die Hinzunahme der allgemeineren n-adischen Zahlen, für welche dieser Satz nicht mehr allgemein gilt, die Untersuchung zunächst wesentlich erschweren; aus diesem Grunde werden in der Folge nur die p-adischen Zahlen untersucht werden, deren Grundzahl eine Primzahl ist.

§ 3. Die Division. Die ganzen und die gebrochenen p-adischen Zahlen.

Unter dem Quotienten $\frac{A}{B}$ zweier p-adischen Zahlen A und B verstehe ich eine Zahl C, welche der Gleichung

(1) $$BC = A \quad (p)$$

genügt. Den Fall $B = 0$ schließen wir von vornherein aus, da er wegen der für jeden Wert von C bestehenden Gleichung $0\cdot C = 0$ nicht zu bestimmten Resultaten führen kann. Ist zunächst der Nenner B eine Einheit, so ist C als eine Zahl unseres Bereiches eindeutig bestimmt. Sind nämlich

$$A = a_0, a_1 a_2 \cdots \quad \text{und} \quad B = b_0, b_1 b_2 \cdots$$

*) Aus der Darstellung (5) ergibt sich auch, wie die weiteren Ziffern von A und B gewählt werden müssen, damit die Gleichung $AB = 0$ (10) mit einer beliebig vorgegebenen Genauigkeit erfüllt ist.

beliebig gegeben, so bestimmen sich die noch unbekannten Ziffern der Zahl

$$C = c_0, c_1 c_2 \cdots \quad (p)$$

aus der Gleichung:

(2) $b_0 c_0 + (b_0 c_1 + b_1 c_0) p + (b_0 c_2 + b_1 c_1 + b_2 c_0) p^2 + \cdots = a_0 + a_1 p + a_2 p^2 + \cdots$.

Durch die Auflösung der Gleichungen:

$$\begin{aligned} b_0 c_0 \qquad\qquad &= a_0 \\ b_1 c_0 + b_0 c_1 \qquad &= a_1 \\ b_2 c_0 + b_1 c_1 + b_0 c_2 &= a_2 \\ \cdots\cdots\cdots \end{aligned}$$

nach den unbekannten Koeffizienten $c_0, c_1, c_2 \ldots$ bestimmen sich diese bekanntlich eindeutig:

$$c_0 = \frac{a_0}{b_0}, \quad c_1 = \frac{a_1 b_0 - a_0 b_1}{b_0^2}, \quad c_2 = \frac{a_0 b_1^2 - a_0 b_0 b_2 - a_1 b_0 b_1 + a_2 b_0^2}{b_0^3}, \ldots,$$

und da die Nenner dieser rationalen Brüche p nicht enthalten, weil sie stets Potenzen von b_0 sind, so sind alle diese Brüche modulo p ganz, d. h. die so sich ergebende Zahl:

$$C = \frac{A}{B} = c_0 + c_1 p + c_2 p^2 + \cdots$$

ist in dem a. S. 24 präzisierten allgemeineren Sinne eine nicht reduzierte p-adische Zahl, welche dann in die ihr gleiche eindeutig bestimmte reduzierte p-adische Zahl übergeführt werden müßte.

Will man aber jenen Quotienten C direkt in der reduzierten Form darstellen, so führt die folgende Überlegung am einfachsten zum Ziele: Schreibt man die rechte Seite der Gleichung (2) in der nicht reduzierten Form:

$$(a_0 + p\varepsilon_1) + (a_1 - \varepsilon_1 + p\varepsilon_2) p + (a_2 - \varepsilon_2 + p\varepsilon_3) p^2 + \cdots,$$

so kann man die modulo p reduzierten Zahlen $c_0, c_1, c_2, \ldots$ und die ganzen Zahlen $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots$ auf eine einzige Weise so bestimmen, daß die Koeffizienten von $1, p, p^2, \ldots$ auf beiden Seiten gleich werden, d. h. daß die Gleichungen erfüllt sind:

$$(3) \qquad \begin{aligned} b_0 c_0 &= a_0 \qquad\; + p\varepsilon_1 \\ b_0 c_1 + b_1 c_0 &= a_1 - \varepsilon_1 + p\varepsilon_2 \\ b_0 c_2 + b_1 c_1 + b_2 c_0 &= a_2 - \varepsilon_2 + p\varepsilon_3 \\ \cdots\cdots\cdots\cdots \end{aligned}$$

In der Tat erhält man ja durch Auflösung dieses Systems von Gleichungen:

$$c_0 = \frac{a_0 + p\varepsilon_1}{b_0},$$

(3a) $$c_1 = \frac{a_1 - \varepsilon_1 + p\varepsilon_2 - b_1 c_0}{b_0},$$

$$c_2 = \frac{a_2 - \varepsilon_2 + p\varepsilon_3 - (b_1 c_1 + b_2 c_0)}{b_0},$$

$$\cdots\cdots\cdots\cdots,$$

und da b_0 von Null verschieden und durch p nicht teilbar ist, so kann man $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots$ stets ganzzahlig so bestimmen, daß der erste, zweite, ... Bruch eine ganze modulo p reduzierte Zahl ist. Man kann nämlich allgemein c_i in (3a) in der Form schreiben:

(3b) $$c_i = \frac{\alpha_i + p\varepsilon_{i+1}}{b_0},$$

wo α_i aus gegebenen Größen und den schon vor c_i berechneten Zahlen $c_0, \ldots c_{i-1}, \varepsilon_1, \ldots \varepsilon_i$ zusammengesetzt, also bekannt ist, sobald die früheren Gleichungen aufgelöst sind. Da aber b_0 und p teilerfremd sind, so kann man bekanntlich durch das sogenannte Euklidische Verfahren zur Bestimmung des größten gemeinschaftlichen Teilers, zwei Multiplikatoren c und ε so bestimmen, daß

$$cb_0 - \varepsilon p = 1$$

ist; multipliziert man diese Gleichung noch mit α_i und setzt:

$$c\alpha_i = \bar{c}_i, \qquad \varepsilon\alpha_i = \bar{\varepsilon}_{i+1},$$

so ergibt sich:

(3c) $$\bar{c}_i b_0 - \bar{\varepsilon}_{i+1} p = \alpha_i.$$

Schreibt man endlich die Gleichung (3c) in der Form:

(3d) $$(\bar{c}_i - \varrho p)\, b_0 - (\bar{\varepsilon}_{i+1} - \varrho b_0)\, p = c_i b_0 - \varepsilon_{i+1} p = \alpha_i,$$

so kann man noch den Multiplikator ϱ eindeutig so bestimmen, daß $\bar{c}_i - \varrho p = c_i$ modulo p reduziert wird, und damit ist dann die obige Gleichung (3b) vollständig gelöst, d. h. c_i und ε_{i+1} den gestellten Bedingungen gemäß bestimmt.

Es gibt also stets eine Zahl C, welche der Gleichung (1) genügt. Man erkennt aber auch leicht, daß es nur eine solche Zahl geben kann. Existierte nämlich noch eine Zahl C' unseres Bereiches, welche der Gleichung (1) genügt, so würde ja:

$$BC = BC' = A \qquad (p)$$

sein, und hieraus folgert man sofort:

$$BC - BC' = B(C - C') = 0 \qquad (p).$$

Da nun B nach Voraussetzung von Null verschieden ist, so muß

$$C - C' = 0 \quad \text{oder} \quad C = C' \qquad (p)$$

sein.

Die praktische Ausführung der Division geschieht genau so wie bei Dezimalbrüchen; nur muß auch hier die Operation bei den Anfangsgliedern a_0 und b_0 beginnen und dann sukzessive von links nach rechts fortgeführt werden. Um die Division von $a_0, a_1 a_2 \ldots$ durch $b_0, b_1 b_2 \ldots$ durchzuführen, dividiere man zunächst a_0 durch b_0, d. h. man bestimme, am leichtesten durch Probieren, die reduzierte Zahl c_0, für welche $b_0 c_0 \equiv a_0 \pmod{p}$ ist, bilde dann die Differenz $A - B c_0$ oder ausgeführt:

$$\begin{array}{rlll} & a_0, & a_1 & a_2 \ldots \\ - & b_0 c_0, & b_1 c_0 & b_2 c_0 \ldots \\ \hline & 0, & a_1' & a_2' \ldots, \end{array} \qquad (p)$$

und behandle diese Differenz dann genau in derselben Weise weiter. So ist z. B. für die Grundzahl 5:

$$\begin{array}{l} 3,12 : 4,21 = 2,4220\,\overline{4220}\ldots \qquad (5) \\ \underline{3\ 03} \\ \ \ 1444\ldots \\ \ \ \underline{1111} \\ \ \ \ 33344\ldots \\ \ \ \ \underline{303} \\ \ \ \ \ 3044\ldots \\ \ \ \ \ \underline{303} \\ \ \ \ \ \ 01444\ldots \\ \ \ \ \ \ \underline{1111} \\ \ \ \ \ \ \ 33344\ldots \\ \ \ \ \ \ \ \ \cdot\ \cdot\ \cdot\ \cdot\ \cdot, \end{array}$$

und man sieht, wie beiläufig bemerkt werden mag, daß dieser Quotient periodisch ist.

Aus der Gleichung $BC = A$ folgt unmittelbar, daß der Quotient $C = \frac{A}{B}$ eine Einheit ist, wenn auch der Zähler eine solche ist. Es gilt also der Satz:

Das Produkt und der Quotient zweier Einheiten ist wieder eine Einheit.

Sind dagegen A und B keine Einheiten, ist also etwa:

$$A = p^{\alpha} E, \quad B = p^{\beta} E'$$

und definiert man den Quotienten $\frac{A}{B}$ wieder durch die Gleichung (1), so ergibt sich jetzt, daß die Gleichung

$$BC = A$$

oder

$$p^{\beta} E' C = p^{\alpha} E$$

durch

$$C = p^{\alpha - \beta} \frac{E}{E'}$$

erfüllt wird. Ist die Ordnung β des Nenners nicht größer als die des Zählers, so findet sich also der Quotient zweier Zahlen A und B auch dann noch in unserem Bereiche, wenn der Nenner keine Einheit ist. Ist aber $\beta > \alpha$, so gibt es dann und nur dann eine Größe, welche gleich $\frac{A}{B}$ ist, wenn wir auch Zahlen von negativer Ordnung, d. h. Größen von der Form

$$(4) \qquad D = \frac{d_{-\varrho}}{p^{\varrho}} + \frac{d_{-(\varrho-1)}}{p^{\varrho-1}} + \cdots + \frac{d_{-1}}{p} + d_0 + d_1 p + d_2 p^2 + \cdots$$

unserem Bereiche adjungieren, deren Koeffizienten wieder modulo p reduzierte ganze Zahlen sind.

Wir wollen dies tun und alle bisher eingeführten Begriffe auf diese neue Klasse von Zahlen übertragen. Sie besitzen also eine negative Ordnungszahl, und wir können sie in der Form:

$$(4\text{a}) \qquad D = p^{-\varrho} E$$

schreiben, wo E wieder eine Einheit und ϱ eine ganze positive Zahl ist. Auch sie wollen wir abgekürzt in der Form:

$$(4\text{b}) \qquad D = d_{-\varrho} d_{-(\varrho-1)} \cdots d_{-1} d_0, d_1 d_2 \cdots \quad (p)$$

schreiben, und sie ebenfalls p-adische Zahlen nennen. Wir nennen diese aber gebrochene p-adische Zahlen, während die bisher allein betrachteten Größen

$$A = a_0 + a_1 p + a_2 p^2 + \cdots = a_0, a_1 a_2 \ldots$$

ganze p-adische Zahlen heißen sollen. Die gebrochenen p-adischen Zahlen unterscheiden sich also nur dadurch von den ganzen, daß sie mehr als eine Ziffer links vom Komma haben. Jede ganze Zahl kann in der Form einer gebrochenen Zahl geschrieben werden, indem man eine beliebige Anzahl von Nullen links vom Komma hinzufügt, d. h.

$$A = 0\,0 \cdots a_0, a_1 a_2 \cdots$$

setzt.

Wir wollen die rationalen Brüche:

$$
(5)\quad
\begin{aligned}
D_{-\varrho} &= d_{-\varrho}\,0\cdots \quad 0,\,0\,0\cdots = \frac{d_{-\varrho}}{p^\varrho},\\
D_{-(\varrho-1)} &= d_{-\varrho}\,d_{-(\varrho-1)}0\cdots 0,\,0\,0\cdots = \frac{d_{-\varrho}}{p^\varrho} + \frac{d_{-(\varrho-1)}}{p^{\varrho-1}},\\
&\vdots\\
D_0 &= d_{-\varrho}\,d_{-(\varrho-1)}\cdots d_0,\,0\,0\cdots = \frac{d_{-\varrho}}{p^\varrho} + \frac{d_{-(\varrho-1)}}{p^{\varrho-1}} + \cdots + d_0,\\
D_1 &= d_{-\varrho}\,d_{-(\varrho-1)}\cdots d_0,\,d_1 0\cdots = \frac{d_{-\varrho}}{p^\varrho} + \frac{d_{-(\varrho-1)}}{p^{\varrho-1}} + \cdots + d_0 + d_1 p,\\
&\vdots
\end{aligned}
$$

welche man durch Fortlassung aller bzw. auf $d_{-\varrho}, d_{-(\varrho-1)}\ldots$ folgenden Ziffern in der Gleichung (4b) für D erhält, als die Näherungswerte $(-\varrho)^{\text{ter}}$, $-(\varrho-1)^{\text{ter}}\ldots$ Ordnung von der gebrochenen p-adischen Zahl D bezeichnen. Dieselben bilden eine wohldefinierte Reihe rationaler Brüche mit dem Nenner p^ϱ, welche für jedes positive oder negative k durch die Gleichung:

$$D_k = D_{k-1} + d_k\cdot p^k \qquad (k = -(\varrho-1),\ -(\varrho-2),\cdots)$$

miteinander zusammenhängen. Auch jetzt gilt also für jedes noch so große k eine Gleichung:

$$D = D_k + p^{k+1}\overline{D}_k \quad (p),$$

wo $p^{k+1}\overline{D}_k$ eine Zahl ist, deren Ordnung mindestens gleich $(k+1)$ ist. Es gilt also für die gebrochenen Zahlen unseres Bereiches der Satz:

Eine gebrochene p-adische Zahl ist zwar selbst im allgemeinen kein positiver rationaler Bruch, sie wird aber mit jeder vorgegebenen Genauigkeit durch einen positiven rationalen Bruch dargestellt, und zwar ist der Nenner genau p^ϱ, wenn diese Zahl die Ordnung $-\varrho$ besitzt. Auch hier gilt also die Gleichung:

$$(6)\qquad D = \lim_{k=\infty} D_k.$$

Wir wollen den $(-1)^{\text{ten}}$ Näherungswert einer gebrochenen Zahl:

$$
(7)\qquad
\begin{aligned}
D_{-1} &= d_{-\varrho}\,d_{-(\varrho-1)}\cdots d_{-1}\,0,\,0\,0\cdots\\
&= \frac{d_{-\varrho}}{p^\varrho} + \frac{d_{-(\varrho-1)}}{p^{\varrho-1}} + \cdots + \frac{d_{-1}}{p},
\end{aligned}
$$

d. h. die Summe der mit negativen Potenzen von p multiplizierten Glieder „den Hauptteil von D für den Bereich von p" nennen; dieser Hauptteil ist für alle ganzen Zahlen Null, für die gebrochenen ein positiver echter Bruch, und aus der Gleichung:

$$D = D_{-1} + d_0, d_1 d_2 \cdots$$

folgt, daß jede gebrochene Zahl unseres Bereiches gleich ihrem Hauptteil vermehrt um eine ganze Zahl ist.

Auch zwei gebrochene Zahlen D und D' heißen kongruent für den Modul p^{k+1}, wenn ihre k^{ten} Näherungswerte D_k und D_k' einander gleich sind, und zwar soll diese Definition sowohl für positive wie für negative Werte des Exponenten k gelten. Aus den unter der Voraussetzung $D_k = D_k'$ bestehenden Gleichungen

$$D = D_k + p^{k+1}\bar{D}_k, \qquad D' = D_k + p^{k+1}\bar{D}_k'$$

folgt sofort durch Subtraktion:

$$D - D' = p^{k+1}(\bar{D}_k - \bar{D}_k').$$

Zwei gebrochene Zahlen sind also dann und nur dann modulo p^{k+1} kongruent, wenn ihre Differenz ein ganzes Vielfaches von p^{k+1} oder durch p^{k+1} teilbar ist.

So sind zum Beispiel für den Bereich von 5 die beiden Zahlen:

$$D = 3210,2 \quad \text{und} \quad D' = 3222,\overline{431}\,431 \cdots$$

einander modulo $\frac{1}{5}$ kongruent, denn es ist:

$$D = 3200,00 \cdots + \left(\frac{1}{5} + 2 \cdot 5\right), \qquad (5)$$

$$D' = 3200,00 \cdots + \left(\frac{2}{5} + 2 + 4 \cdot 5 + 3 \cdot 5^2 + \cdots\right) \qquad (5),$$

und ihre Differenz ist wirklich ein ganzes Vielfaches von $\frac{1}{5}$, wie auch die Ausführung der Subtraktion lehrt:

$$\begin{array}{r} {}^{54444} \\ 3210,2 \\ -\ 3222,431431\cdots \\ \hline 42,213013\ldots \end{array}$$

Wir weisen noch darauf hin, daß die gebrochenen Zahlen unseres Bereiches nicht übereinstimmen mit den gebrochenen Zahlen der gewöhnlichen Zahlenlehre. Denn wir nennen hier eine Zahl gebrochen oder ganz, für den Bereich von p, je nachdem sie von negativer Ordnung ist oder nicht, oder was dasselbe ist, je nachdem ihre Näherungswerte negative Potenzen von p enthalten oder nicht. Ein rationaler reduzierter Bruch $\frac{A}{B}$ ist also für den Bereich von p gebrochen oder ganz, je nachdem sein Nenner durch p teilbar ist oder nicht.

Wir wollen jetzt die Gesamtheit aller ganzen und gebrochenen p-adischen Zahlen den zu p gehörigen Zahlkörper nennen und ihn durch $K(p)$ bezeichnen.

Dann folgt aus den bis jetzt durchgeführten Betrachtungen, daß dieser Bereich $K(p)$ so groß ist, daß in ihm die vier elementaren Rechenoperationen der Addition, Subtraktion, Multiplikation und Division unbeschränkt ausgeführt werden können, die letzte allerdings nur unter der selbstverständlichen Bedingung, daß der Divisor von Null verschieden ist. Die einfachen Regeln für die Ausführung dieser Operationen bleiben auch für die gebrochenen Zahlen unverändert bestehen; nur muß man bei der Multiplikation und Division mit Zahlen von positiver oder negativer Ordnung das Komma um so viel Stellen nach rechts oder nach links verschieben, als die Ordnungszahl des Multiplikators oder Divisors Einheiten enthält.

Für die Division wollen wir noch einige weitere Bemerkungen anfügen: Ist der Divisor $B = p^{\beta} E'$ keine Einheit, so dividiert man zunächst durch E' und multipliziert das so erhaltene Resultat noch mit $p^{-\beta}$, wodurch man den gesuchten Quotienten $\frac{A}{B}$ erhält.

Wie bei der Addition, Subtraktion und Multiplikation können wir auch bei der Division den Quotienten als den Grenzwert der aus den Näherungswerten gebildeten Brüche definieren, d. h.

$$\frac{A}{B} = \lim_{k=\infty} \left(\frac{A_k}{B_k}\right) \qquad (p)$$

setzen. Ist nämlich $C = \frac{A}{B}$, also $A = BC$, so ergibt sich durch Übergang zu den Näherungswerten für jedes k die Kongruenz:

$$B_k \cdot C_k \equiv A_k \pmod{p^{k+1}}$$

oder

$$B_k\left(C_k - \frac{A_k}{B_k}\right) \equiv 0 \pmod{p^{k+1}}.$$

Ist nun B, also auch B_k von der Ordnung β, so ist die letzte Kongruenz nur möglich, wenn $C_k - \frac{A_k}{B_k}$ durch $p^{k-\beta+1}$ teilbar ist. Es ist also für jedes noch so große k

$$C_k \equiv \frac{A_k}{B_k} \pmod{p^{k-\beta+1}},$$

d. h. C ist dann und nur dann gleich dem Quotienten $\frac{A}{B}$, wenn für jede noch so hohe Potenz p^M von p als Modul die Kongruenz besteht,

$$C_k \equiv \frac{A_k}{B_k} \pmod{p^M},$$

sobald man hinreichend genaue Näherungswerte wählt, d. h. sobald k genügend groß ist. Man muß eben k mindestens gleich $M + \beta - 1$ wählen.

Auf Grund der hiermit nachgewiesenen Gleichung:

$$C = \frac{A}{B} = \lim_{k=\infty} \left(\frac{A_k}{B_k}\right) \qquad (p)$$

bleibt also unsere Definition der Gleichheit bestehen, wonach zwei Zahlen dann und nur dann gleich heißen, wenn ihre Näherungswerte für jede noch so hohe Potenz von p kongruent sind, sobald man nur ihre Ordnung genügend groß wählt.

Verbinden wir eine endliche Anzahl von Zahlen des Körpers $K(p)$ durch die elementaren Rechenoperationen, so erhalten wir einen rationalen Ausdruck $R(A, B, C, \cdots D)$, der wieder eine Zahl unseres Körpers darstellt. Diese Zahl ist dadurch eindeutig definiert, daß

$$R = R(A, B, C, \cdots D) = \lim_{k=\infty} R(A_k, B_k, C_k, \cdots D_k) \qquad (p)$$

ist. Denn es besteht ja auch hier der Satz, daß

$$(8) \qquad R_k \equiv R(A_k, B_k, \cdots D_k) \pmod{p^M}$$

ist, wo M eine Zahl bedeutet, die mit k beliebig groß wird. Die Kongruenz (8) gilt zwar nicht immer für den Modul p^{k+1}, da sich, wie wir oben gesehen haben, bei der Division die Ordnung des Kongruenzmoduls erniedrigen kann; auf jeden Fall erniedrigt sie sich aber nur um eine bestimmte endliche Anzahl von Einheiten, sodaß sie durch Vergrößerung von k trotzdem beliebig groß gemacht werden kann.

§ 4. Der Körper $K(p)$ der p-adischen Zahlen und der Körper $K(1)$ der rationalen Zahlen.

Auch die rationalen Zahlen bilden einen in sich abgeschlossenen Bereich, dessen Elemente sich durch die vier elementaren Operationen wiedererzeugen. Jeden solchen abgeschlossenen Bereich nennen wir nach Dedekind einen Körper und wir wollen diesen durch $K(1)$ bezeichnen, weil er alle und nur die Zahlen umfaßt, welche aus der Zahl 1 durch die beliebig aber endlich oft angewandten Operationen der Addition, Subtraktion, Multiplikation und Division entstehen. Jede Zahl des Körpers $K(1)$, d. h. jeder rationale positive oder negative Bruch, ist für den Bereich von p gleich einer Zahl des Körpers $K(p)$, wie wir soeben bewiesen haben. Das Umgekehrte ist aber, wie wir gleich zeigen werden, nicht der Fall, und wir wollen deshalb den Körper $K(1)$ als einen Teilkörper von $K(p)$ bezeichnen.

Wir wollen nun untersuchen, wie eine Zahl des Körpers $K(p)$ beschaffen sein muß, damit sie für den Bereich von p gleich einem rationalen Bruche ist, also dem Teilkörper $K(1)$ angehört. Diese Aufgabe wird vollständig durch den folgenden Satz gelöst:

Eine Zahl des Bereiches $K(p)$ ist dann und nur dann für den Bereich von p gleich einer rationalen Zahl, wenn sie periodisch ist.

Zunächst wissen wir, daß die ganzen positiven Zahlen und nur sie durch abbrechende Reihen dargestellt werden. Schreiben wir sie formal als unendliche Reihen, so erhalten sie die Periode 0. Die ganzen negativen Zahlen erhält man, indem man die entsprechende positive ganze Zahl von der Null subtrahiert. Ist $A = a_0, a_1 a_2 \cdots a_\varrho$, so ist die zugehörige negative Zahl:

$$-A = (p-a_0), (p-1-a_1)(p-1-a_2)\cdots(p-1-a_\varrho)\,(p-1)\,(p-1)\cdots.$$

Jede negative ganze Zahl ist also periodisch mit der Periode $(p-1)$; und offenbar ist auch umgekehrt jede solche Zahl für den Bereich von p einer negativen ganzen Zahl gleich.

Wir haben also den Beweis nur noch für die rationalen Brüche zu führen. Hierbei können wir uns von vornherein auf die für den Bereich von p ganzen und rein periodischen Zahlen

(1) $$x = \overline{a_0, a_1 a_2 \cdots a_{\nu-1}}\; \overline{a_0 a_1 \cdots a_{\nu-1}} \cdots \quad (p)$$

beschränken, denn jede für den Bereich von p gebrochene Zahl kann ja durch Multiplikation mit einer geeigneten Potenz von p ganz gemacht, und eine gemischt periodische Zahl

$$b_0, b_1 \ldots b_{\sigma-1}\, \overline{a_0 a_1 \ldots a_{\nu-1}} \ldots$$

kann durch Subtraktion der ganzen positiven Zahl $b_0, b_1 \ldots b_{\sigma-1}$ und darauf folgende Division durch p^σ auf die Form (1) gebracht werden. Schließlich dürfen wir annehmen, daß die obige ν-gliedrige Periode die kleinste ist, die x besitzt. Dann folgt aus Gleichung (1) nach Multiplikation mit p^ν:

$$p^\nu x = 0, 0 \cdots 0\, \overline{a_0 a_1 \cdots a_{\nu-1}} \cdots \quad (p),$$

und hieraus durch Subtraktion von (1):

$$x(1-p^\nu) = a_0, a_1 \cdots a_{\nu-1} = m = a_0 + a_1 p + \cdots + a_{\nu-1} p^{\nu-1},$$

wo m eine unterhalb $p^\nu - 1$ liegende gewöhnliche ganze Zahl ist; nur dann wäre nämlich $m = p^\nu - 1$, wenn alle $a_i = p - 1$ wären, und das ist mit der Annahme nicht verträglich, daß die Zahl x in (1) keine Periode von weniger als ν Gliedern besitzen sollte. Also ist:

$$x = -\frac{m}{p^\nu - 1} \quad (p),$$

also ein negativer echter Bruch, und zwar ist $p^\nu - 1$ offenbar die kleinste unter den Zahlen $p^{\bar{\nu}} - 1$, für welche die Zahl $x(1-p^{\bar{\nu}})$ ganz ist, weil anderenfalls x eine kürzere Periode haben würde. Ist umgekehrt:

$$x = -\frac{m_1}{n_1}$$

ein negativer echter Bruch in seiner reduzierten Form, dessen Nenner p nicht enthält, und gehört p modulo n_1 zum Exponenten ν, so daß

$$p^\nu - 1 = n_1 \bar{n}$$

ist, so besteht die Gleichung:

$$x = -\frac{m_1 \bar{n}}{p^\nu - 1} = \frac{m}{1 - p^\nu} = m(1 + p^\nu + p^{2\nu} + \cdots), \qquad (p)$$

wo $m = a_0 + a_1 p + \cdots + a_{\nu-1} p^{\nu-1}$ gesetzt werden kann, weil $m < p^\nu - 1$ ist. Also ergibt sich für den beliebig angenommenen negativen echten Bruch x, falls dieser modulo p ganz ist, eine p-adische Darstellung von der Form:

$$x = \overline{a_0, a_1 \cdots a_{\nu-1}}\ \overline{a_0 a_1 \cdots a_{\nu-1}} \cdots.$$

Jeder negative echte Bruch, welcher in seiner reduzierten Form p nicht im Nenner enthält, ist also für den Bereich von p einer rein periodischen p-adischen Zahl gleich, und umgekehrt ist jede rein periodische p-adische Zahl gleich einem solchen rationalen Bruche.

Da aber jeder andere rationale Bruch aus einem solchen echten Bruche durch Multiplikation mit einer Potenz von p und durch Hinzufügung einer positiven oder einer negativen ganzen Zahl hervorgeht, so ist jeder rationale Bruch gleich einer rein oder gemischt periodischen p-adischen Zahl, und umgekehrt jede periodische p-adische Zahl einem rationalen Bruche gleich. Wir können daher den Satz aussprechen:

Der Teilbereich $K(1)$ von $K(p)$ enthält alle und nur die periodischen reduzierten p-adischen Zahlen.

§ 5. Untersuchung der nicht reduzierten p-adischen Zahlen in bezug auf ihre Größe. Die p-adische Darstellung der rationalen Zahlen.

Die reduzierten p-adischen Zahlen sind reine Symbole, mit denen nach bestimmten Vorschriften zu rechnen ist, und die aufgestellte Definition der Gleichheit zweier p-adischen Zahlen ist von der gewöhnlichen Definition dieses Begriffes vollständig verschieden.

Betrachten wir aber neben den reduzierten auch die nicht reduzierten p-adischen Zahlen, so gibt es unter ihnen auch solche Reihen:

$$\bar{a}_0 + \bar{a}_1 p + \bar{a}_2 p^2 + \cdots,$$

welche im gewöhnlichen Sinne, d. h. ihrer Größe nach, gegen einen bestimmten Grenzwert konvergieren; sind z. B. die Koeffizienten $\bar{a}_i$ hinreichend schnell abnehmende rationale Brüche, deren Nenner p nicht

enthalten, so sind diese Zahlen modulo p ganz, und jene Reihe besitzt also ihrer Größe nach einen bestimmten endlichen Wert, während sie für den Bereich von p nach der a. S. 24 oben gemachten Bemerkung einer ebenfalls bestimmten p-adischen Zahl gleich ist.

Ist z. B. n eine beliebige durch p nicht teilbare Zahl, welche größer als p ist, und a eine modulo p ganze rationale Zahl, so ist die nicht reduzierte p-adische Zahl:

$$a + a\,\frac{p}{n} + a\left(\frac{p}{n}\right)^2 + \cdots$$

dem rationalen Bruche

$$\frac{a}{1 - \frac{p}{n}}$$

sowohl der Größe nach, als auch für den Bereich von p gleich, weil ihr k^{ter} Näherungswert

$$a\left(1 + \frac{p}{n} + \cdots + \left(\frac{p}{n}\right)^k\right) = a \cdot \frac{1 - \left(\frac{p}{n}\right)^{k+1}}{1 - \frac{p}{n}}$$

sich von jenem rationalen Bruche um die Zahl

$$a \cdot \frac{\left(\frac{p}{n}\right)^{k+1}}{1 - \frac{p}{n}}$$

unterscheidet, welche mit wachsendem k sowohl der Größe nach, als auch für den Bereich von p beliebig klein gemacht werden kann. So stellt z. B. die unendliche Reihe:

$$\frac{1}{5} + \frac{1}{5}\left(\frac{2}{5}\right) + \frac{1}{5}\left(\frac{2}{5}\right)^2 + \cdots$$

den Bruch $\frac{1}{3}$ sowohl der Größe nach, als auch für den Bereich von 2 dar, d. h. ihre Näherungswerte genügend hoher Ordnung unterscheiden sich von $\frac{1}{3}$ um beliebig kleine reduzierte Brüche, deren Zähler durch eine beliebig hohe Potenz von 2 teilbar sind.

Ich werde zeigen, daß und wie man alle rationalen und auch alle algebraischen Zahlen so in konvergente p-adische Reihen entwickeln kann, daß sie diese sowohl ihrer Größe nach als auch für den Bereich der Primzahl p mit jeder vorgegebenen Genauigkeit darstellen, und daß jede rationale Gleichung mit rationalen Koeffizienten, welche der Größe nach zwischen ihnen besteht, auch für den Bereich von p erfüllt ist, und umgekehrt.

Zunächst beweise ich aber den wichtigen Satz, daß man eine beliebige rationale oder irrationale Zahl B stets so in eine konvergente p-adische Reihe entwickeln kann, daß diese für den Bereich von p einer ganz beliebig vorgegebenen reduzierten p-adischen Zahl:

$$\bar{B} = \bar{b}_0 + \bar{b}_1 p + \bar{b}_2 p^2 + \cdots \tag{1}$$

gleich wird. So besitzt z. B. eine rationale Zahl B unendlich viele konvergente p-adische Entwicklungen, aber nur eine unter ihnen ist auch für den Bereich von p gleich derselben Zahl B, und nur diese werden wir später eben die p-adische Darstellung dieser rationalen Zahl B nennen.

Man findet leicht Reihen, welche ihrer Größe nach gegen einen ganz anderen Grenzwert konvergieren, als für den Bereich von p. So konvergiert z. B. die Reihe

$$\frac{2}{3} + \frac{2^2}{13} + \frac{2^3}{313} + \frac{2^4}{195313} + \cdots \tag{2}$$

d. h. die unendliche Reihe

$$\sum_1^{\infty} \frac{2^k}{a_k}, \text{ wo } a_1 = 3 \text{ und } a_{k+1} = 2a_k(a_k - 1) + 1 \tag{2a}$$

ist, ihrer Größe nach gegen 1, wie eine leichte Rechnung zeigt. In der Tat ergibt sich aus der obigen Rekursionsformel:

$$a_{k+1} = 2^{k+1} a_1 a_2 \cdots a_k + 1,$$

und hieraus folgt auf induktivem Wege, daß der k^{te} Näherungswert unserer Reihe

$$S_k = \frac{2}{a_1} + \frac{2^2}{a_2} + \cdots + \frac{2^k}{a_k} = 1 - \frac{1}{a_1 \cdots a_k}$$

sein muß, da unter dieser Annahme für ein bestimmtes k wirklich

$$\begin{aligned} S_{k+1} &= 1 - \frac{1}{a_1 \cdots a_k} + \frac{2^{k+1}}{a_{k+1}} = 1 - \frac{a_{k+1} - 2^{k+1} a_1 \cdots a_k}{a_1 \cdots a_k a_{k+1}} \\ &= 1 - \frac{1}{a_1 \cdots a_{k+1}} \end{aligned}$$

sich ergibt, und die Gleichung für $k = 1$ erfüllt ist. Während diese Reihe also ihrer Größe nach gegen 1 konvergiert, ist sie für den Bereich der Primzahl 2 gleich der reduzierten dyadischen Zahl

$$0,1\,0\,0\,0\,1\,0\,0\,1 \cdots = 2 + 2^5 + 2^8 + \cdots \quad (2),$$

also sicher nicht gleich Eins. Ferner konvergiert die unendliche Reihe

$$1 + \frac{3}{1} + \frac{3^2}{1 \cdot 2} + \cdots$$

bekanntlich ihrer Größe nach gegen e^3, und eine leichte Rechnung zeigt, daß sie für den Bereich von 3 gleich der reduzierten triadischen Zahl

$$1{,}1\,1\,2\,2\,0\,1\,1\,0\,0\,1\cdots(3)$$

ist.

Die Entwicklung der reellen Zahl B in eine konvergente p-adische Reihe, welche für den Bereich von p gleich der beliebig gegebenen Zahl $\bar{B}$ in (1) ist, kann man nun z. B. folgendermaßen ausführen.

Es sei wieder n eine durch p nicht teilbare Zahl, welche größer als p ist. Ist dann $\frac{\gamma}{n}$ das größte Multiplum von $\frac{1}{n}$, welches gerade noch kleiner ist als B, so bilden die p aufeinander folgenden Brüche:

$$\frac{\gamma}{n},\quad \frac{\gamma-1}{n},\ \ldots\ \frac{\gamma-(p-1)}{n}$$

ein vollständiges Restsystem modulo p, da sie alle modulo p inkongruent sind. Es gibt also unter ihnen einen einzigen Bruch, etwa $\frac{c_0}{n}$, welcher dem nullten Näherungswerte $\bar{b}_0$ der in (1) gegebenen Zahl $\bar{B}$ modulo p kongruent ist. Da ferner das ganze Intervall:

$$\left(\frac{\gamma-(p-1)}{n},\ \ldots\ \frac{\gamma-1}{n},\ \frac{\gamma}{n},\ B\right)$$

höchstens gleich $\frac{p}{n}$ ist, so ist, wo auch der Bruch $\frac{c_0}{n}$ in diesem Intervalle liegen möge:

$$0 < B - \frac{c_0}{n} \leqq \frac{p}{n}.$$

Setzt man also:

$$B = \frac{c_0}{n} + \frac{p}{n}\cdot B_1,$$

so ist B_1 eine positive Zahl, welche höchstens gleich Eins sein kann. In derselben Weise wähle ich jetzt einen neuen Bruch $\frac{c_1}{n}$ so aus, daß

$$0 < B_1 - \frac{c_1}{n} \leqq \frac{p}{n}$$

und daß zugleich:

$$\frac{c_0}{n} + \frac{p}{n}\cdot\frac{c_1}{n} \equiv \bar{b}_0 + \bar{b}_1 p \pmod{p^2}$$

ist, wodurch wieder c_1 nur modulo p bestimmt wird. Fährt man in derselben Weise fort, so erhält man eine Reihe von Gleichungen von der folgenden Form:

$$B = \frac{c_0}{n} + \frac{p}{n} \cdot B_1,$$

(3)
$$B_1 = \frac{c_1}{n} + \frac{p}{n} \cdot B_2,$$
$$\vdots$$
$$B_\varrho = \frac{c_\varrho}{n} + \frac{p}{n} \cdot B_{\varrho+1},$$

wo allgemein
$$0 < B_i \leq 1 \qquad (i = 1, 2, \cdots \varrho + 1)$$
ist, und wo die Zähler c_i so bestimmt sind, daß allgemein:

(4) $$\frac{c_0}{n} + \frac{c_1}{n}\left(\frac{p}{n}\right) + \frac{c_2}{n}\left(\frac{p}{n}\right)^2 + \cdots + \frac{c_i}{n}\left(\frac{p}{n}\right)^i \equiv \bar{b}_0 + \bar{b}_1 p + \cdots + \bar{b}_i p^i \pmod{p^{i+1}}$$
ist.

Aus den Gleichungen (3) ergibt sich also eine Darstellung von B:
$$B = \frac{c_0}{n} + \frac{c_1}{n}\left(\frac{p}{n}\right) + \cdots + \frac{c_\varrho}{n}\left(\frac{p}{n}\right)^\varrho + B_{\varrho+1}\left(\frac{p}{n}\right)^{\varrho+1},$$
in welcher das Glied $B_{\varrho+1}$ positiv und höchstens gleich Eins ist. Da nun n. d. V. $\frac{p}{n} < 1$ ist, so wird das Restglied von B mit wachsendem ϱ unendlich klein; die so bestimmte unendliche p-adische Reihe:
$$\frac{c_0}{n} + \frac{c_1}{n} \cdot \left(\frac{p}{n}\right) + \frac{c_2}{n}\left(\frac{p}{n}\right)^2 + \cdots$$
konvergiert also ihrer Größe nach gegen B. Da ferner die ganzen Zahlen c_k so gewählt sind, daß nach (4) allgemein der i^{te} Näherungswert dieser Reihe, dem i^{ten} Näherungswerte der p-adischen Reihe $\bar{B}$ modulo p^{i+1} kongruent ist, so ist dieselbe p-adische Reihe für den Bereich von p der reduzierten p-adischen Zahl $\bar{B}$ gleich, d. h. es bestehen wirklich die beiden Gleichungen:

(5) $$\sum_0^\infty \frac{c_i}{n}\left(\frac{p}{n}\right)^i = B; \qquad \sum_0^\infty \frac{c_i}{n}\left(\frac{p}{n}\right)^i = \bar{B}, \qquad (p)$$

w. z. b. w.*) Setzt man z. B. $B = \pi$, $\bar{B} = 0$, $n = 100$, $p = 3$, so ergibt eine leichte Rechnung, daß schon die vier ersten Glieder der nicht reduzierten triadischen Reihe:
$$\frac{312}{100} + \frac{70}{100} \cdot \frac{3}{100} + \frac{65}{100} \cdot \left(\frac{3}{100}\right)^2 + \frac{27}{100} \cdot \left(\frac{3}{100}\right)^3 + \cdots$$
der Größe nach die Zahl π bis zur siebenten Stelle, dagegen für den Bereich von 3 die Null genau bis zur dritten Stelle ergeben.

Die hier angegebene Darstellung kann natürlich mannigfach abgeändert werden; in jedem Falle ist aber die sich ergebende unendliche Reihe sowohl ihrer Größe nach als auch für den Bereich von p durch

*) Durch eine völlig analoge Rechnung kann man diese Aufgabe offenbar auch in dem Falle lösen, wenn die gegebene p-adische Zahl
$$\bar{B} = \bar{b}_k p^k + \bar{b}_{k+1} p^{k+1} + \cdots$$
von beliebiger positiver oder negativer Ordnung ist.

die Forderung eindeutig bestimmt, daß sie der Größe nach gegen B für den Bereich von p gegen $\bar{B}$ konvergieren soll.

Ganz ebenso beweist man, daß auch jede komplexe Zahl $B + Ci$ in eine konvergente p-adische Reihe

$$(6) \qquad B + Ci = \frac{b_0 + c_0 i}{n} + \frac{b_1 + c_1 i}{n}\left(\frac{p}{n}\right) + \frac{b_2 + c_2 i}{n}\left(\frac{p}{n}\right)^2 + \cdots$$

mit komplexen Koeffizienten so entwickelt werden kann, daß sie für den Bereich von p einer beliebigen reduzierten p-adischen Zahl:

$$\bar{B} = \bar{b}_0 + \bar{b}_1 p + \bar{b}_2 p^2 + \cdots$$

gleich wird. Setzt man nämlich in (6) die reellen und die imaginären Bestandteile einander gleich, so ergeben sich die beiden reellen Gleichungen:

$$\sum \frac{b_k}{n} \cdot \left(\frac{p}{n}\right)^k = B, \qquad \sum \frac{c_k}{n} \cdot \left(\frac{p}{n}\right)^k = C.$$

Wählt man nun die Koeffizienten b_k und c_k nach der soeben angegebenen Methode so aus, daß diese beiden Gleichungen erfüllt sind, und daß außerdem:

$$\sum \frac{b_k}{n}\left(\frac{p}{n}\right)^k = \bar{B} = \sum \bar{b}_k p^k, \qquad (p)$$
$$\sum \frac{c_k}{n}\left(\frac{p}{n}\right)^k = 0 \qquad (p)$$

ist, so ist den beiden Forderungen genügt, und auch hier ist die Reihe (6) sowohl ihrer Größe nach, als auch für den Bereich von p eindeutig bestimmt.

Jede reelle oder komplexe Zahl kann also so in eine konvergente p-adische Reihe entwickelt werden, daß sie für den Bereich von p einer beliebig gegebenen p-adischen Zahl gleich wird.

Es seien nun:

$$\beta = \sum b_i p^i, \qquad \gamma = \sum c_i p^i$$

zwei konvergente p-adische Reihen, und zwar möge der Größe nach:

$$\beta = B, \qquad \gamma = C$$

sein, während für den Bereich von p:

$$\beta = \bar{B}, \qquad \gamma = \bar{C} \qquad (p)$$

sein soll. Alsdann ist nach unserer Definition der elementaren Rechenoperationen für den Bereich von p:

$$\beta \pm \gamma = \sum (b_i \pm c_i)\, p^i = \bar{B} \pm \bar{C} \qquad (p),$$
$$\beta\gamma = b_0 c_0 + p\,(b_0 c_1 + b_1 c_0) + \cdots = \bar{B}\bar{C} \qquad (p),$$
$$\frac{\beta}{\gamma} = \frac{b_0}{c_0} + \frac{b_0 c_1 - b_1 c_0}{c_0^{\,2}} + \cdots = \frac{\bar{B}}{\bar{C}} \qquad (p).$$

Dieselben Reihen konvergieren aber bekanntlich auch ihrer Größe nach, und zwar gegen die Zahlen: $B \pm C$, BC und $\frac{B}{C}$. Natürlich muß bei der Division der Fall, daß $\bar{C}$ oder C gleich Null ist, ausgeschlossen werden.

Sind also β und γ zwei konvergente p-adische Reihen, welche der Größe nach gleich B und C, für den Bereich von p gleich $\bar{B}$ und $\bar{C}$ sind, so sind $\beta \pm \gamma$, $\beta\gamma$, $\frac{\beta}{\gamma}$ ebenfalls konvergente p-adische Reihen, welche der Größe nach gegen $B \pm C$, BC, $\frac{B}{C}$, und für den Bereich von p gegen $\bar{B} \pm \bar{C}$, $\bar{B}\bar{C}$, $\frac{\bar{B}}{\bar{C}}$ konvergieren.

Durch Verallgemeinerung dieser Resultate folgt endlich der Satz:

Haben β und γ die oben angegebene Bedeutung und ist $\varphi(x, y)$ eine beliebige rationale Funktion von x und y mit rationalen Zahlkoeffizienten, so ist stets:

$$\varphi(\beta, \gamma) = \varphi(B, C),$$
$$\varphi(\beta, \gamma) = \varphi(\bar{B}, \bar{C}) \quad (p),$$

wobei nur der Fall auszuschließen ist, daß der Nenner von $\varphi(x, y)$ für $x = B$, $y = C$ der Größe nach, oder für $x = \bar{B}$, $y = \bar{C}$ für den Bereich von p verschwindet.

Ich betrachte jetzt speziell die positiven und negativen rationalen Zahlen. Jede solche Zahl B kann, wie wir sahen, auf unendlich viele Arten in eine konvergente p-adische Reihe entwickelt werden, so nämlich, daß sie außerdem einer beliebigen reduzierten oder auch nicht reduzierten p-adischen Zahl $\bar{B}$ für den Bereich von p gleich wird. Unter diesen Entwicklungen wähle ich nun stets diejenige und bezeichne sie allein als die p-adische Darstellung der rationalen Zahl B, welche auch für den Bereich von p derselben rationalen Zahl B gleich ist. Ist also

$$\beta = \sum b_i p^i$$

diese p-adische Entwicklung der rationalen Zahl B, so ist sie sowohl ihrer Größe nach als auch für den Bereich von p eindeutig durch die beiden Gleichungen:

$$\beta = B \quad (p), \qquad \beta = B$$

charakterisiert. So ist z. B. die a. S. 40 angegebene geometrische Reihe die p-adische Darstellung der rationalen Zahl $\frac{a}{1 - \frac{p}{n}}$; dagegen

ist die Reihe (2) a. S. 41 nicht die dyadische Darstellung der Zahl 1, weil sie für den Bereich von 2 nicht gleich Eins ist. Natürlich gibt es unendlich viele formal verschiedene p-adische Darstellungen derselben rationalen Zahl B, jedoch sind sie alle sowohl der Größe nach als auch für den Bereich von p einander gleich, können also ineinander übergeführt werden.

Eine rationale Gleichung:

$$\varphi(x) = 0$$

mit rationalen Zahlkoeffizienten ist dann und nur dann für die p-adische Entwicklung

$$x = \beta = \sum b_i p^i$$

der rationalen Zahl B erfüllt, wenn dieselbe Gleichung auch für den Bereich von p besteht und umgekehrt, und dies ist stets und nur dann der Fall, wenn $\varphi(B) = 0$ ist.

In der Tat konvergiert ja die Zahl $\varphi(\beta) = \varphi(\sum b_i p^i)$ sowohl der Größe nach, als auch für den Bereich von p gegen denselben Grenzwert, nämlich gegen die rationale Zahl $\varphi(B)$ und diese ist dann und nur dann der Größe nach Null, wenn das Gleiche für den Bereich von p der Fall ist. Genau ebenso wird endlich der folgende allgemeinere Satz bewiesen:

Eine rationale Gleichung:

$$\varphi(x, y, \cdots z) = 0$$

mit rationalen Zahlkoeffizienten ist dann und nur dann für die p-adischen Entwicklungen:

$$x = \beta = \sum b_i p^i, \qquad y = \gamma = \sum c_i p^i, \quad \cdots z = \delta = \sum d_i p^i$$

der rationalen Zahlen $B, C, \ldots D$ erfüllt, wenn dieselbe Gleichung auch für den Bereich von p besteht und umgekehrt, und dies ist stets und nur dann der Fall, wenn die rationale Zahl $\varphi(B, C, \ldots D) = 0$ ist.

Drittes Kapitel.

Die ganzen rationalen Funktionen mit p-adischen Koeffizienten.

---

§ 1. Definitionen. Der Körper $K(p, x)$ der rationalen Funktionen von x.

Ich betrachte jetzt die ganzen rationalen Funktionen:

(1) $$f(x) = A_0 x^n + A_1 x^{n-1} + \cdots + A_n$$

einer Variablen x mit beliebigen ganzen oder gebrochenen p-adischen Koeffizienten, und gebe für sie zunächst einige Definitionen und Sätze, welche aus den für die p-adischen Zahlen gefundenen Resultaten ohne weiteres hervorgehen.

Die Funktion $f(x)$ heißt ganzzahlig für den Bereich von p, wenn alle Koeffizienten A_i ganze p-adische Zahlen sind. Eine ganzzahlige Funktion $f(x)$ heißt primitiv, wenn nicht alle ihre Koeffizienten A_i durch p teilbar sind, wenn also mindestens einer derselben eine Einheit ist. Jede ganze Funktion $f(x)$ kann auf eine einzige Weise in der Form

(2) $$f(x) = p^\delta \cdot f_0(x)$$

geschrieben werden, wo p^δ die höchste in allen Koeffizienten A_i enthaltene Potenz von p und $f_0(x)$ eine primitive Funktion bedeutet. Dann soll p^δ der Zahlenteiler und $f_0(x)$ die primitive Funktion von $f(x)$ genannt werden. Der Zahlenteiler ist dann und nur dann eine negative Potenz von p, wenn $f(x)$ nicht ganzzahlig ist.

Es sei $f(x)$ eine beliebige ganzzahlige Funktion von x, und es mögen:

(3) $$\begin{aligned} A_0 &= a_0^{(0)},\ a_1^{(0)} a_2^{(0)} \cdots, \\ A_1 &= a_0^{(1)},\ a_1^{(1)} a_2^{(1)} \cdots, \\ &\ \vdots \\ A_n &= a_0^{(n)},\ a_1^{(n)} a_2^{(n)} \cdots \end{aligned} \qquad (p)$$

die Darstellungen ihrer Koeffizienten sein. Ersetzt man dann alle Koeffizienten A_i durch ihre Näherungswerte $A_i^{(k)}$ einer und derselben k^{ten} Ordnung, so erhält man eine ganze Funktion n^{ten} Grades

(4) $$f^{(k)}(x) = A_0^{(k)} x^n + A_1^{(k)} x^{n-1} + \cdots + A_n^{(k)}$$

mit positiven ganzzahligen Koeffizienten, welche der k^{te} Näherungswert von $f(x)$ genannt werden soll. Die so sich ergebenden Näherungswerte

(5) $$\begin{aligned} f^{(0)}(x) &= a_0^{(0)} x^n \quad + a_0^{(1)} x^{n-1} \quad + \cdots + a_0^{(n)}, \\ f^{(1)}(x) &= a_0^{(0)}, a_1^{(0)} x^n + a_0^{(1)}, a_1^{(1)} x^{n-1} + \cdots + a_0^{(n)}, a_1^{(n)} \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

bilden eine wohldefinierte Reihe von ganzen Funktionen mit positiven Zahlkoeffizienten, für welche dieselben Definitionen und Sätze gelten, wie für die Näherungswerte der p-adischen Zahlen.

Zwei Funktionen $f(x)$ und $\bar{f}(x)$ heißen kongruent für den Modul p^{k+1}, wenn ihre k^{ten} Näherungswerte $f^{(k)}(x)$ und $\bar{f}^{(k)}(x)$ noch übereinstimmen, oder, was dasselbe ist, wenn alle entsprechenden Koeffizienten A_i und $\bar{A}_i$ modulo p^{k+1} kongruent sind. Zwei Funktionen heißen gleich für den Bereich von p, wenn ihre Näherungswerte genügend hoher Ordnung für jede noch so hohe Potenz von p kongruent, d. h. wenn ihre entsprechenden Koeffizienten beziehlich gleich sind.

Sind $f^{(0)}(x), f^{(1)}(x), \ldots$ die sukzessiven Näherungswerte von $f(x)$, so ist allgemein:

(6) $$f^{(k+1)}(x) = f^{(k)}(x) + p^{k+1}\,\mathfrak{f}^{(k+1)}(x),$$

wo:

(6a) $$\mathfrak{f}^{(k+1)}(x) = a_{k+1}^{(0)} x^n + a_{k+1}^{(1)} x^{n-1} + \cdots + a_{k+1}^{(n)}$$

das Aggregat aller Glieder von $f(x)$ ist, die mit p^{k+1} multipliziert sind, und diese Gleichung läßt sich als Kongruenz in der Form:

$$f^{(k+1)}(x) \equiv f^{(k)}(x) \pmod{p^{k+1}}$$

schreiben. Allgemeiner besteht auch für ein beliebiges k die Kongruenz:

$$f(x) \equiv f^{(k)}(x) \pmod{p^{k+1}},$$

weil ja eben der k^{te} Näherungswert von $f(x)$ mit $f^{(k)}(x)$ identisch ist. Wir können also auch hier:

$$f(x) = \lim_{k=\infty} (f^{(k)}(x)) \qquad (p)$$

setzen.

Eine ganzzahlige Funktion $f_0(x)$ ist offenbar dann und nur dann primitiv, besitzt also keinen Zahlenteiler, wenn ihr nullter Näherungswert

$$f_0^{(0)}(x) = a_0^{(\lambda)} x^\lambda + \cdots + a_0^{(0)} \qquad (a_0^{(\lambda)} > 0)$$

nicht Null ist. Ist $g_0(x)$ eine andere primitive Funktion, ist also auch ihr nullter Näherungswert:

$$g_0^{(0)}(x) = b_0^{(\mu)} x^\mu + \cdots + b_0^{(0)} \qquad (b_0^{(\mu)} > 0)$$

von Null verschieden, so ist auch ihr Produkt $h_0(x) = f_0(x) g_0(x)$ primitiv, denn für den nullten Näherungswert dieses Produktes besteht die Kongruenz:

$$h_0^{(0)}(x) \equiv f_0^{(0)}(x)\, g_0^{(0)}(x) \equiv a_0^{(\lambda)} b_0^{(\mu)} x^{\lambda+\mu} + \cdots \pmod{p},$$

und hier ist der Koeffizient $a_0^{(\lambda)} b_0^{(\mu)}$ von $x^{\lambda+\mu}$ durch p sicher nicht teilbar, wenn $a_0^{(\lambda)}$ und $b_0^{(\mu)}$, wie vorausgesetzt wurde, nicht Null sind. Es ergibt sich also der Satz:

Das Produkt zweier primitiven Funktionen ist wieder primitiv. Sind λ und μ die Grade der nullten Näherungswerte der Faktoren, so ist der Grad des nullten Näherungswertes ihres Produktes gleich $\lambda + \mu$.

Sind

$$f(x) = p^\delta f_0(x), \qquad g(x) = p^\varepsilon g_0(x)$$

zwei beliebige ganze Funktionen, $f_0(x)$ und $g_0(x)$ die zugehörigen primitiven Funktionen, so ist:

$$f(x)\, g(x) = p^{\delta+\varepsilon} f_0(x)\, g_0(x) = p^{\delta+\varepsilon} h_0(x),$$

und da $h_0(x)$ wieder primitiv ist, so ergibt sich der allgemeinere Satz:

Der Zahlenteiler eines Produktes ist gleich dem Produkte der Zahlenteiler seiner Faktoren.

Die Gesamtheit aller rationalen ganzen oder gebrochenen Funktionen mit p-adischen Koeffizienten bildet offenbar auch einen Bereich oder Körper, dessen Individuen sich durch die elementaren Rechnungsoperationen wiedererzeugen, denn die Summe, die Differenz, das Produkt und der Quotient von zwei rationalen Funktionen ist wieder eine solche. Ich bezeichne diesen Körper kurz durch $K(p, x)$. Analog soll $K(1, x)$ die Gesamtheit, oder den Körper aller rationalen Funktionen von x mit gewöhnlichen rationalen Brüchen, d. h. mit Zahlen von $K(1)$ als Koeffizienten bedeuten. Auch hier ist $K(1, x)$ ein Teilkörper von $K(p, x)$, denn er enthält ja alle und nur die Funktionen von $K(p, x)$, deren Koeffizienten periodisch sind.

§ 2. Die einfachen und mehrfachen Gleichungswurzeln. Das Euklidische Verfahren zur Bestimmung des größten gemeinsamen Teilers.

Für die ganzen Funktionen mit p-adischen Koeffizienten gelten offenbar alle Resultate und Methoden der elementaren Algebra, soweit diese nur die vier elementaren Rechenoperationen voraussetzen, weil

diese ja für die p-adischen Zahlen genau ebenso wie für die gewöhnlichen Zahlen definiert sind. Es sollen daher nur die wichtigsten von diesen Sätzen kurz angegeben werden.

Eine ganze Funktion $f(x) = A_0 x^n + A_1 x^{n-1} + \cdots + A_n$ des Bereiches $K(p, x)$ läßt sich stets nach Potenzen eines beliebigen Linearfaktors $x - \xi$ entwickeln, wenn ξ eine beliebige p-adische Zahl bedeutet. Ersetzt man nämlich in $f(x)$ die Variable x durch $\xi + (x - \xi)$, so ergibt sich allein mit Hilfe des binomischen Lehrsatzes:

$$(1)\quad f(x) = f(\xi + \overline{x - \xi}) = f(\xi) + \frac{f'(\xi)}{1!}(x-\xi) + \frac{f''(\xi)}{2!}(x-\xi)^2 + \cdots + \frac{f^{(n)}(\xi)}{n!}(x-\xi)^n \quad (p),$$

wenn allgemein $f^{(i)}(\xi)$ der Wert der i^{ten} Ableitung von $f(x)$ für $x = \xi$ ist.

Eine p-adische Zahl ξ heißt eine **Wurzel** der Gleichung

$$(2)\qquad f(x) = 0, \qquad (p)$$

wenn die p-adische Zahl $f(\xi)$ für den Bereich von p gleich Null ist, d. h. wenn ihre Näherungswerte von genügend hoher Ordnung durch jede noch so hohe Potenz von p teilbar sind.

So besitzt z. B. die Gleichung:

$$f(x) = x^2 + 1 = 0 \qquad (5)$$

die beiden Wurzeln:

$$x_1 = 2, 1\,2\,1\,3\,4 \cdots, \qquad x_2 = 3, 3\,2\,3\,1\,0 \cdots,$$

welche durch ein der Wurzelausziehung aus Dezimalbrüchen durchaus entsprechendes Verfahren beliebig weit eindeutig bestimmt werden können. Die Gleichung

$$x^2 - 2 = 0 \qquad (5)$$

besitzt für den Bereich von (5) keine Wurzel, während die kubische Gleichung:

$$f(x) = x^3 - 2 = 0 \qquad (5)$$

die eine Wurzel: $\sqrt[3]{2} = 3, 0\,2\,2\,1 \cdots$ hat, welche ebenfalls nach Analogie der gewöhnlichen Methode beliebig weit berechnet werden kann.

Dagegen besitzt diese Gleichung keine weitere pentadische Wurzel; wir werden später zeigen, daß und wie der Bereich der pentadischen Zahlen erweitert werden muß, damit sie ihrem Grade entsprechend genau drei Wurzeln habe.

Aus der Darstellung (1) folgt nun genau wie in der elementaren Algebra der Satz:

Besitzt die Gleichung $f(x) = 0$ die Wurzel $x = \xi$, so ist ihre linke Seite durch den zugehörigen Linearfaktor $(x - \xi)$ teilbar.

In der Tat folgt ja aus (1) unter der Voraussetzung $f(\xi) = 0$:

$$(3) \qquad f(x) = (x - \xi)\left(f'(\xi) + \frac{f''(\xi)}{2!}(x - \xi) + \cdots\right) = (x - \xi)\, f_1(x),$$

wo $f_1(x)$ eine ganze Funktion des $(n-1)^{\text{ten}}$ Grades mit p-adischen Koeffizienten ist. So ist z. B. identisch:

$$x^2 + 1 = (x - 2{,}12134\cdots)(x - 3{,}32310\cdots), \qquad (5)$$

$$x^3 - 2 = (x - 3{,}0221\cdots)(x^2 + 3{,}0221\cdots x + 4{,}1240\cdots). \qquad (5)$$

In jedem Falle kann man den komplementären Divisor $f_1(x)$ durch gewöhnliche Division oder aus der Gleichung:

$$\frac{f(x)}{x - \xi} = \frac{f(x) - f(\xi)}{x - \xi} = A_0 x^{n-1} + (A_0 \xi + A_1)\, x^{n-2} + (A_0 \xi^2 + A_1 \xi + A_2)\, x^{n-3} + \cdots \qquad (p)$$

finden.

Die Zahl ξ heißt eine h-fache Wurzel der Gleichung

$$f(x) = 0 \qquad (p),$$

wenn ihre linke Seite genau durch $(x - \xi)^h$ teilbar ist; dies ist, wie aus (1) unmittelbar hervorgeht, dann und nur dann der Fall, wenn $f(x)$ selbst und ihre $(h-1)$ ersten Ableitungen für $x = \xi$ verschwinden, während $f^{(h)}(\xi)$ von Null verschieden ist. Im folgenden soll immer eine h-fache Wurzel als äquivalent h gleichen einfachen Wurzeln angesehen werden. Besitzt die Gleichung $f(x) = 0$ die h-fache Wurzel ξ, so folgt aus (1), daß

$$f(x) = (x - \xi)^h \left(\frac{f^{(h)}(\xi)}{h!} + \frac{f^{(h+1)}(\xi)}{(h+1)!}(x - \xi) + \cdots\right) = (x - \xi)^h f_1(x) \qquad (p),$$

ist, wo $f_1(x)$ eine ganze Funktion des $(n-h)^{\text{ten}}$ Grades ist, welche den Linearfaktor $(x - \xi)$ offenbar nicht mehr enthält. Hieraus geht hervor, daß eine Funktion n^{ten} Grades eine Wurzel höchstens n-fach enthalten kann.

Im Anschluß an diese Betrachtungen beweisen wir den folgenden allgemeinen Satz:

Besitzt die Gleichung $f(x) = 0$ für den Bereich von p die k gleichen oder verschiedenen Wurzeln $\xi_1, \xi_2, \ldots \xi_k$, so ist ihre linke Seite durch das Produkt der k zugehörigen Linearfaktoren $(x - \xi_1)(x - \xi_2)\ldots(x - \xi_k)$ teilbar.

Dieser Satz wurde für $k = 1$ soeben bewiesen, und nach der Definition der mehrfachen Wurzeln gilt er auch für ein beliebiges k, falls

alle k Wurzeln einander gleich sind. Wir nehmen nun an, der Satz sei bereits für einen Wert von k bewiesen; sind dann $\xi_1, \xi_2 \dots \xi_k$ k gleiche oder verschiedene Wurzeln von $f(x) = 0$, so besteht die Gleichung:

(4) $$f(x) = (x - \xi_1)(x - \xi_2) \cdots (x - \xi_k) f_{k+1}(x) \qquad (p).$$

Wir können ferner annehmen, daß jede dieser Wurzeln bereits so oft aufgenommen ist, als sie überhaupt in $f(x)$ vorkommt. Ist dann ξ_{k+1} eine weitere Wurzel unserer Gleichung, so ist diese von allen $\xi_1, \xi_2, \dots \xi_k$ verschieden. Ersetzt man nun in der Gleichung (4) x durch ξ_{k+1}, so folgt:

$$0 = (\xi_{k+1} - \xi_1)(\xi_{k+1} - \xi_2) \cdots (\xi_{k+1} - \xi_k) f_{k+1}(\xi_{k+1}) \qquad (p),$$

und dieses Produkt kann nur dann Null sein, wenn mindestens einer seiner Faktoren gleich Null ist; da jedoch nach der Voraussetzung alle Differenzen $(\xi_{k+1} - \xi_i)$ von Null verschieden sind, so muß $f_{k+1}(\xi_{k+1}) = 0$, d. h. $f_{k+1}(x) = (x - \xi_{k+1}) f_{k+2}(x)$, also wegen (4):

$$f(x) = (x - \xi_1) \cdots (x - \xi_k)(x - \xi_{k+1}) f_{k+2}(x) \qquad (p)$$

sein, und damit ist unsere Behauptung durch den Schluß von k auf $k + 1$ bewiesen.

Besitzt unsere Gleichung speziell n gleiche oder verschiedene Wurzeln: $\xi_1, \xi_2, \dots \xi_n$, so ist also:

(5) $$f(x) = A_0(x - \xi_1)(x - \xi_2) \cdots (x - \xi_n) \qquad (p),$$

wo A_0 offenbar der Koeffizient von x^n in $f(x)$ ist. Da somit $f(x)$ eine $(n + 1)^{\text{te}}$ Wurzel ξ_{n+1} nur dann haben kann, wenn in der Identität (5) $A_0 = 0$ ist, so ergibt sich endlich der Satz:

> Eine Gleichung n^{ten} Grades kann innerhalb des Bereiches $K(p)$ nicht mehr als n Wurzeln haben, es sei denn, daß alle ihre Koeffizienten Null sind.

Auch die Lehre von der Teilbarkeit der ganzen Funktionen können wir in vollem Umfange für den Bereich $K(p)$ der p-adischen Zahlen entwickeln, da sie nur die elementaren Rechenoperationen voraussetzt. Eine Funktion $f(x)$ heißt teilbar durch eine andere $\delta(x)$, wenn $f(x) = \delta(x) f_1(x)$ und $f_1(x)$ ebenfalls eine ganze Funktion ist. Durch einfache Division kann man sich stets überzeugen, ob $\delta(x)$ in $f(x)$ enthalten ist oder nicht.

Zwei ganze Funktionen $f(x)$ und $g(x)$ besitzen den gemeinsamen Teiler $\delta(x)$, wenn $\delta(x)$ sowohl in $f(x)$ als in $g(x)$ enthalten ist. Alle gemeinsamen Teiler $\delta(x)$ von $f(x)$ und $g(x)$ sind die sämtlichen Divisoren ihres größten gemeinsamen Teilers $d(x)$; dieser kann bekanntlich durch das sogenannte Euklidische Verfahren zur Aufsuchung des größten gemeinsamen Teilers bestimmt werden. Indem ich die bezüglichen Beweise als bekannt voraussetze, will ich das Verfahren selbst

kurz angeben: $f(x)$ und $g(x)$ seien bzw. vom Grade μ und ν, und es sei $\mu \geqq \nu$. Ich bilde dann durch sukzessive Divisionen die Gleichungen:

$$\begin{aligned} f(x) &= g(x)\,g_1(x) + h(x), \\ g(x) &= h(x)\,h_1(x) + k(x), \\ h(x) &= k(x)\,k_1(x) + l(x), \qquad (p) \\ &\vdots \\ q(x) &= r(x)\,r_1(x) + s(x), \\ r(x) &= s(x)\,s_1(x), \end{aligned} \tag{6}$$

wo z. B. $g_1(x)$ der Quotient und $h(x)$ der Rest der Division von $f(x)$ durch $g(x)$ ist. Da die Grade der Reste $h(x)$, $k(x)$, $l(x), \ldots$ beständig abnehmen, muß man nach einer endlichen Anzahl von Divisionen zu einem Abschlusse kommen, und man zeigt dann leicht, daß der letzte von Null verschiedene Divisionsrest $s(x) = d(x)$ der gesuchte größte gemeinsame Teiler von $f(x)$ und $g(x)$ ist. Ist dieser Teiler $d(x)$ vom nullten Grade, also eine Zahl, so heißen $f(x)$ und $g(x)$ teilerfremd oder relativ prim.

Schreibt man die Gleichungen (6) in der Form:

$$\begin{aligned} h(x) &= f(x) - g(x)\,g_1(x), \\ k(x) &= g(x) - h(x)\,h_1(x), \qquad (p) \\ &\cdots\cdots\cdots \\ s(x) &= q(x) - r(x)\,r_1(x), \end{aligned} \tag{6a}$$

so erhält man durch sukzessive Elimination von $h(x)$, $k(x), \ldots$ zuletzt eine lineare homogene Darstellung des größten gemeinsamen Teilers $s(x) = d(x)$ durch $f(x)$ und $g(x)$, welche sich in der Form schreiben läßt:

$$f(x)\,\bar{g}(x) + g(x)\,\bar{f}(x) = d(x) \qquad (p). \tag{7}$$

Sind also $f(x)$ und $g(x)$ zwei beliebige ganze Funktionen und $d(x)$ ihr größter gemeinsamer Teiler für den Bereich von p, so kann man stets zwei Multiplikatoren $\bar{f}(x)$ und $\bar{g}(x)$ so bestimmen, daß die Gleichung (7) identisch erfüllt ist.

Sind speziell $f(x)$ und $g(x)$ teilerfremd, also ihr größter gemeinsamer Teiler $d(x) = d$ eine Zahl, so kann man die Gleichung (7) durch d dividieren. Ersetzt man dann die Multiplikatoren $\frac{\bar{f}(x)}{d}$ und $\frac{\bar{g}(x)}{d}$ wieder durch $\bar{f}(x)$ und $\bar{g}(x)$, so ergibt sich der speziellere Satz:

Sind $f(x)$ und $g(x)$ zwei teilerfremde ganze Funktionen, so kann man zwei Multiplikatoren $\bar{f}(x)$ und $\bar{g}(x)$ auf rationalem Wege so bestimmen, daß:

$$f(x)\,\bar{g}(x) + g(x)\,\bar{f}(x) = 1 \tag{7a}$$

ist.

§ 3. Die Resultante zweier Funktionen.

Mit Hilfe der im vorigen Abschnitt gefundenen Resultate wollen wir nun einen aus den Koeffizienten zweier Funktionen

$$(1)\qquad \begin{aligned} f(x) &= A_0 x^{\mu} + A_1 x^{\mu-1} + \cdots + A_{\mu}, \\ g(x) &= B_0 x^{\nu} + B_1 x^{\nu-1} + \cdots + B_{\nu} \end{aligned}$$

gebildeten Ausdruck $R(f, g)$ angeben, dessen Verschwinden die notwendige und hinreichende Bedingung dafür ist, daß jene beiden Funktionen einen gemeinsamen Teiler haben; dieser Ausdruck wird **die Resultante** jener beiden Funktionen genannt und ist für unsere weiteren Betrachtungen von besonderer Wichtigkeit.

Die beiden Funktionen $f(x)$ und $g(x)$ besitzen dann und nur dann einen gemeinsamen Teiler, wenn man zwei Multiplikatoren $f_1(x)$ und $g_1(x)$ von niedrigerem als dem μ^{ten} bzw. ν^{ten} Grade so bestimmen kann, daß

$$(2)\qquad f(x)\,g_1(x) + g(x)\,f_1(x) = 0 \qquad (p)$$

ist.

Ist nämlich $d(x)$ jener gemeinsame Teiler, und setzt man:

$$f(x) = d(x)\,f_1(x), \qquad g(x) = -\,d(x)\,g_1(x),$$

so ergibt sich durch Elimination von $d(x)$ unmittelbar die obige Gleichung. Besteht umgekehrt jene Gleichung (2), und nehmen wir an, $f(x)$ und $g(x)$ seien teilerfremd, so kann man, wie oben gezeigt wurde, zwei andere Multiplikatoren $\bar{f}(x)$ und $\bar{g}(x)$ so bestimmen, daß

$$(2\text{a})\qquad f(x)\,\bar{g}(x) + g(x)\,\bar{f}(x) = 1 \qquad (p)$$

ist. Eliminiert man nun aus (2) und (2a) $f(x)$, so würde sich:

$$(2\text{b})\qquad g(x)\,(f_1(x)\,\bar{g}(x) - g_1(x)\,\bar{f}(x)) = -\,g_1(x) \qquad (p)$$

ergeben, und es müßte also entweder $g_1(x)$ durch $g(x)$ teilbar sein, was unmöglich ist, da $g_1(x)$ höchstens vom $\nu - 1^{\text{ten}}$ Grade ist, oder es müßte der Koeffizient von $g(x)$ in (2b) gleich Null sein, aber auch dies ist unmöglich, da ja dann auch $g_1(x)$ gleich Null sein würde.

Es seien nun

$$(3)\qquad \begin{aligned} f_1(x) &= C_0 x^{\mu-1} + C_1 x^{\mu-2} + \cdots + C_{\mu-1}, \\ g_1(x) &= D_0 x^{\nu-1} + D_1 x^{\nu-2} + \cdots + D_{\nu-1} \end{aligned}$$

zwei noch unbekannte Funktionen des $\mu - 1^{\text{ten}}$ bzw. $\nu - 1^{\text{ten}}$ Grades; sucht man dann die Koeffizienten C_i und D_k so zu bestimmen, daß die Gleichung (2) identisch erfüllt wird, so erhält man für diese $\mu + \nu$ Koeffizienten ebensoviele lineare homogene Gleichungen:

$$
(4)\qquad \begin{array}{lll}
A_0 D_0 & + B_0 C_0 & = 0, \\
A_1 D_0 + A_0 D_1 & + B_1 C_0 + B_0 C_1 & = 0, \\
\dots & \dots & \dots \\
\dots & \dots & \dots
\end{array}
$$

welche besagen, daß die Koeffizienten von $x^{\mu+\nu-1}$, $x^{\mu+\nu-2}, \dots x, 1$ einzeln gleich Null sein müssen. Da aber ein System solcher Gleichungen dann und nur dann durch nicht sämtlich verschwindende Werte der Unbekannten C_i, D_k befriedigt werden kann, wenn ihre Determinante gleich Null ist, so gibt das Verschwinden jener Determinante die notwendige und hinreichende Bedingung für die Existenz eines gemeinsamen Teilers von $f(x)$ und $g(x)$, ist also die gesuchte Resultante.

Vertauscht man in ihr noch die Zeilen und Kolonnen, so kann die Eliminationsresultante der beiden Funktionen $f(x)$ und $g(x)$ folgendermaßen geschrieben werden:

$$
(5)\qquad R(f, g) = \begin{vmatrix}
A_0, & A_1, \dots A_\mu & 0 \dots\dots 0 \\
0 & A_0, A_1 \dots A_\mu & \dots\dots 0 \\
\vdots & & \\
0 & 0 \dots 0 & A_0, A_1 \dots\dots A_\mu \\
B_0, & B_1, \dots\dots & B_\nu \; 0 \dots 0 \\
0 & B_0, B_1 \dots\dots & B_\nu \dots 0 \\
\vdots & & \\
0 & 0 \dots 0 & B_0, B_1 \dots\dots B_\nu
\end{vmatrix}
\begin{array}{l}
\left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} (\nu \text{ Zeilen}) \\
\left.\begin{array}{l} \\ \\ \\ \\ \end{array}\right\} (\mu \text{ Zeilen})
\end{array}
$$

Aus dieser Darstellung der Resultante ziehe ich zunächst einige Folgerungen, welche später benutzt werden sollen. Es sei speziell

$$f(x) = x - \xi$$

eine lineare Funktion, also

$$A_0 = 1, \quad A_1 = -\xi, \quad \mu = 1.$$

Dann ist:

$$
(5\text{a})\qquad R(x - \xi, g(x)) = \begin{vmatrix}
1, & -\xi & 0 & \dots\dots & 0 \\
0 & 1, & -\xi & \dots\dots & 0 \\
\vdots & & & & \\
0 & 0 & 0 & \dots\dots & 1, -\xi \\
B_0 & B_1 & B_2 & \dots & B_{\nu-1}, \; B_\nu
\end{vmatrix}.
$$

Man erkennt sehr leicht, daß der Wert der rechts stehenden Determinante gleich $g(\xi)$ ist; addiert man nämlich die mit ξ multiplizierte erste Kolonne zur zweiten, addiert man hierauf die mit ξ multiplizierte zweite Kolonne zur dritten und fährt so fort, so fallen zuletzt alle Elemente

$-\xi$ rechts von der Diagonalreihe fort, und die Determinante erhält den Wert:

$$R((x-\xi), g(x)) = \begin{vmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & \dots & 1 & 0 \\ \bar{B}_0 & \bar{B}_1 & \bar{B}_2 & \dots & \bar{B}_{\nu-1} & \bar{B}_\nu \end{vmatrix} = \bar{B}_\nu,$$

wo allgemein $\bar{B}_i$ der Wert ist, in den B_i durch jene Umformungen übergeht. Da aber offenbar

$$\bar{B}_\nu = B_0\xi^\nu + B_1\xi^{\nu-1} + \dots + B_\nu = g(\xi)$$

wird, so ergibt sich wirklich:

$$R(x-\xi, g(x)) = g(\xi). \tag{6}$$

In der Tat ist ja $g(\xi)$ stets und nur dann Null, wenn $x-\xi$ und $g(x)$ den gemeinsamen Teiler $x-\xi$ haben.

Einen besonders wichtigen speziellen Fall der Resultanten erhält man, wenn man annimmt, daß die zweite Funktion

$$g(x) = f'(x) = \mu A_0 x^{\mu-1} + (\mu-1)A_1 x^{\mu-2} + \dots + A_{\mu-1}$$

die Ableitung der ersten ist. Diese Resultante:

$$Rf((x), f'(x)) = \begin{vmatrix} A_0 \dots\dots A_\mu \; 0 \dots\dots 0 \\ 0 \; A_0 \dots\dots A_\mu \dots 0 \\ \dots\dots\dots\dots\dots\dots \\ 0 \; 0 \dots A_0 \dots\dots\dots A_\mu \\ \mu A_0 \dots A_{\mu-1} \; 0 \dots 0 \\ 0 \; \mu A_0 \dots\dots A_{\mu-1} \dots 0 \\ \ddots \\ 0 \; 0 \dots \mu A_0 \dots A_{\mu-1} \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}(\mu-1)\text{ Zeilen} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\}\mu\text{ Zeilen} \end{matrix} \tag{7}$$

nennt man die **Diskriminante** der **Funktion** $f(x)$ und bezeichnet sie durch $D(f(x))$. Sie verschwindet also dann und nur dann, wenn $f(x)$ mit seiner Ableitung einen gemeinsamen Teiler hat, und dies tritt immer ein, wenn $f(x)$ auch nur einen quadratischen Faktor besitzt. Denn ist dies der Fall, und ist

$$f(x) = (d(x))^2 f_1(x),$$

so ist ja die Ableitung

$$f'(x) = 2d(x)\,d'(x)\,f_1(x) + (d(x))^2 f_1'(x)$$

offenbar durch $d(x)$ ebenfalls teilbar, d. h. es ist wirklich

$$R(f(x), f'(x)) = 0.$$

§ 4. Elementare Eigenschaften der Resultanten und Diskriminanten.

Ich gebe zuerst einige einfache Eigenschaften der Resultante $R(f, g)$ an, welche sich aus der Natur der sie darstellenden Determinante (5) a. S. 55 fast unmittelbar ablesen lassen.

I. Vertauscht man in dieser Determinante die erste Funktion $f(x)$ mit der zweiten $g(x)$, so ergibt sich sofort

(1) $$R(g, f) = (-1)^{\mu\nu} R(f, g),$$

denn dieser Vertauschung entsprechen offenbar in jener Determinante $\mu\nu$ Zeilenvertauschungen.

II Es sei ferner $\nu > \mu$; bildet man dann die Eliminationsresultante

$$R(f(x), g(x) + cx^{\nu-\mu-\lambda} f(x))$$

der beiden Funktionen:

$$f(x) = A_0 x^\mu + A_1 x^{\mu-1} + \cdots + A_\mu,$$
$$\bar{g}(x) = g(x) + cx^{\nu-\mu-\lambda} f(x) = B_0 x^\nu + \cdots + (B_\lambda + cA_0)x^{\nu-\lambda} +$$
$$+ (B_{\lambda+1} + cA_1)x^{\nu-\lambda-1} + \cdots,$$

wo λ eine der Zahlen $0, 1, \ldots \nu - \mu$ bedeuten kann, so unterscheiden sich die Koeffizienten von $\bar{g}(x)$ von den entsprechenden von $g(x)$ nur dadurch, daß $B_\lambda, B_{\lambda+1}, \ldots B_{\lambda+\mu}$ bzw. um $cA_0, cA_1, \ldots cA_\mu$ vermehrt sind. Die Determinante für $R(f, \bar{g})$ geht also einfach dadurch aus $R(f, g)$ in (5) hervor, daß zu der ersten, zweiten, ... μ^{ten} Zeile der B bzw. die mit c multiplizierte $(\lambda+1)^{\text{te}}, (\lambda+2)^{\text{te}}, \ldots (\lambda+\mu)^{\text{te}}$ Zeile der A addiert wird. Da aber diese Operationen den Wert einer Determinante nicht ändern, so ergibt sich die Gleichung:

$$R(f(x), g(x) + cx^{\nu-\mu-\lambda} f(x)) = R(f(x), g(x)).$$

Es sei jetzt allgemeiner

$$h(x) = C_0 x^{\nu-\mu} + C_1 x^{\nu-\mu-1} + \cdots + C_{\nu-\mu}$$

eine beliebige ganze Funktion von nicht höherem als dem $(\nu-\mu)^{\text{ten}}$ Grade. Dann folgt aus dem soeben bewiesenen Satze sofort, daß:

(2) $$R(f(x), g(x) + h(x) f(x)) = R(f(x), g(x))$$

ist, denn man braucht diesen Satz nur für

$$\lambda = 0, 1, \ldots \nu - \mu$$

sukzessive anzuwenden, um die Richtigkeit der letzten Gleichung zu beweisen. Derselbe Satz gilt auch, wenn $h(x)$ eine ganze Funktion beliebigen Grades von x ist, nur tritt in diesem Falle noch eine gewisse Potenz von A_0 bzw. B_0 als Faktor auf; der einfache Beweis dieser Tatsache, welcher ganz analog geführt wird, mag dem Leser überlassen bleiben.

III. Fast ebenso einfach kann die folgende dritte Eigenschaft der Resultante bewiesen werden.

Sind

$$h(x) = H_0 x^\alpha + H_1 x^{\alpha-1} + \cdots + H_\alpha,$$
$$k(x) = K_0 x^\vartheta + K_1 x^{\vartheta-1} + \cdots + K_\vartheta$$

zwei beliebige Funktionen, so besteht die Gleichung:

(3) $$R(h(x)k(x),\ g(x)) = R(h(x),\ g(x)) \cdot R(k(x),\ g(x)).$$

Zum Beweise dieses Satzes stellen wir (nach dem Vorgange von E. Netto Algebra § 152) die beiden auf der rechten Seite von (3) stehenden Resultanten als Determinanten $(\alpha+\beta+\nu)^{\text{ter}}$ Ordnung dar und beweisen, daß ihr nach dem Multiplikationssatze gebildetes Produkt der linksstehenden Resultante gleich ist. Es ist nämlich:

$$B_\nu^\vartheta \cdot R(h(x), g(x)) = \left|\begin{array}{llllll} H_0 \ldots\ldots & H_\alpha \ldots & & & & \\ \vdots & & & & & \\ 0 \ldots & H_0 \ldots\ldots & H_\alpha \ldots\ldots\ldots & & & \\ B_0 \ldots\ldots & B_\nu \ldots\ldots\ldots & & & & \\ \vdots & & & & & \\ 0 \ldots & B_0 \ldots\ldots & B_\nu \ldots\ldots\ldots & & & \\ 0 & 0 \ldots\ldots & 0 & B_\nu & & \\ & & & & \ddots & \\ 0 \ldots & 0 \ldots\ldots & 0 & & & B_\nu \end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{l}a\\a\\a\end{array}}\right\} \nu \text{ Zeilen} \\ \left.\vphantom{\begin{array}{l}a\\a\\a\end{array}}\right\} \alpha \text{ Zeilen} \\ \left.\vphantom{\begin{array}{l}a\\a\\a\end{array}}\right\} \beta \text{ Zeilen} \end{array}$$

denn die rechtsstehende Determinante geht ja aus der Determinante für $R(h(x), g(x))$ durch Ränderung mit β Zeilen und Kolonnen hervor, welche nur in der Diagonale das Element B_ν und sonst lauter Nullen enthalten. Ebenso leicht erkennt man, daß:

$$K_0^\alpha \cdot R(k(x), g(x)) = \left|\begin{array}{llllll} K_0 \ldots & K_\vartheta & & & & \\ & K_0 \ldots\ldots & K_\vartheta & & & \\ & & \ddots & & & \\ & & K_0 \ldots\ldots & K_\vartheta & & \\ & & & K_0 \ldots\ldots & K_\vartheta & \\ & & & & \ddots & \\ & & & & K_0 \ldots & K_\vartheta \\ & & & B_0 \ldots\ldots & B_\nu & \\ & & & & \ddots & \\ & & & & B_0 \ldots\ldots & B_\nu \end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{l}a\\a\\a\\a\end{array}}\right\} \alpha \text{ Zeilen} \\ \left.\vphantom{\begin{array}{l}a\\a\\a\end{array}}\right\} \nu \text{ Zeilen} \\ \left.\vphantom{\begin{array}{l}a\\a\\a\end{array}}\right\} \beta \text{ Zeilen} \end{array}$$

ist, denn hier ist die aus den $(\nu + \beta)$ letzten Zeilen und Kolonnen gebildete Unterdeterminante gleich $R(k(x),\ g(x))$, und an sie schließen sich nach links und nach oben die α rändernden Spalten und Zeilen an.

Bildet man nun das Produkt dieser beiden Determinanten in der gewöhnlichen Weise, daß die Zeilen der ersten mit den Kolonnen der zweiten multipliziert werden, so erhält man eine Determinante der $(\alpha+\beta+\nu)^{\text{ten}}$ Ordnung, deren erste ν Zeilen völlig mit denjenigen der Resultante von

$$h(x)\,k(x) = H_0K_0x^{\alpha+\beta} + (H_0K_1 + H_1K_0)x^{\alpha+\beta-1} + \cdots + H_\alpha K_\beta$$

und $g(x)$ übereinstimmen, aber auch die $\alpha+\beta$ letzten Zeilen können leicht durch Zeilenverbindungen unter Heraussetzung von $K_0^\alpha B_\nu^\beta$ in die entsprechenden Zeilen jener Resultante $R(h(x)\,k(x),\,g(x))$ verwandelt werden. Und damit ist jener Satz vollständig bewiesen.

Wegen des Vertauschungssatzes (I) besteht dieselbe Gleichung auch in dem Falle, daß die zweite Funktion $g(x)$ gleich dem Produkte zweier Faktoren niedrigeren Grades ist, und der Satz läßt sich offenbar auch auf den Fall von mehr als zwei Faktoren ausdehnen.

Ich gebe zuerst einige einfache Anwendungen dieses wichtigen Satzes: Ist $f(x) = (f_0(x))^s$ die Potenz einer anderen Funktion, so folgt aus dem soeben bewiesenen Theorem:

(4) $$R(f_0(x)^s,\ g(x)) = R(f_0(x),\ g(x))^s,$$

also speziell für $f_0(x) = x - \xi$, nach (6) a. S. 56

(4a) $$R((x-\xi)^s,\ g(x)) = g(\xi)^s.$$

Besonders einfach wird der Ausdruck für die Resultante zweier Funktionen, von denen die eine, etwa die erste, in lauter Linearfaktoren zerfällt. Ist nämlich

$$f(x) = (x-\xi_1)(x-\xi_2)\cdots(x-\xi_\mu),$$

so ergibt sich aus dem Satze (3):

(5) $$\begin{aligned} R(f(x),\ g(x)) &= R\Big(\prod_i (x-\xi_i),\ g(x)\Big) = \prod_i R(x-\xi_i,\ g(x)) \\ &= \prod_i g(\xi_i) = g(\xi_1)\,g(\xi_2)\cdots g(\xi_\mu). \end{aligned}$$

Ist auch $g(x)$ gleich dem Produkte von ν Linearfaktoren, ist also:

$$g(x) = B_0(x-\eta_1)(x-\eta_2)\cdots(x-\eta_\nu),$$

so ergibt die soeben gefundene Formel

$$R(f(x),\ g(x)) = B_0^\mu\cdot\prod_{i=1}^{\mu}\prod_{k=1}^{\nu}(\xi_i-\eta_k).$$

Nehmen wir auch in $f(x)$ den Koeffizienten A_0 nicht gleich Eins an, so folgt unter Anwendung des Vertauschungssatzes (1) leicht das allgemeine Theorem:

Die Resultante zweier in Linearfaktoren zerlegbarer Funktionen:

$$f(x) = A_0(x - \xi_1) \cdots (x - \xi_\mu),\ g(x) = B_0(x - \eta_1) \cdots (x - \eta_\nu)$$

ist durch die einfachen Gleichungen

$$(6)\quad \begin{aligned} R(f(x),\ g(x)) &= A_0^\nu B_0^\mu \prod_{i=1}^{\mu} \prod_{k=1}^{\nu} (\xi_i - \eta_k) = A_0^\nu \cdot \prod_{i=1}^{\mu} g(\xi_i) \\ &= (-1)^{\mu\nu} \cdot B_0^\mu \prod_{k=1}^{\nu} f(\eta_k) \end{aligned}$$

gegeben.

Bei diesen Darstellungen sieht man ohne weiteres, daß $R(f, g)$ dann und nur dann verschwindet, wenn $f(x)$ und $g(x)$ mindestens einen Linearfaktor gemeinsam haben, d. h. wenn mindestens ein $\xi_i = \eta_k$ ist. Auch die vorher durch allerdings sehr einfache Determinantenbetrachtungen bewiesenen drei fundamentalen Eigenschaften der Resultante werden in diesem Falle alle trivial. Erst später werden wir beweisen, daß jede Funktion $f(x)$ mit beliebigen p-adischen Koeffizienten auf eine einzige Weise in ein Produkt p-adischer Linearfaktoren $x - \xi_i$ zerlegt werden kann. Da wir aber den Beweis dafür gerade unter Benutzung jener drei Eigenschaften der Resultante führen werden, so wurden diese hier auf direktem Wege erwiesen.

Ein für die folgenden Untersuchungen besonders wichtiges Resultat erhält man, wenn man die soeben bewiesenen Sätze auf die Diskriminanten anwendet, welche ja spezielle Resultanten sind.

Ist

$$f(x) = h(x)\, k(x)$$

eine Funktion n^{ten} Grades, welche gleich dem Produkt zweier Faktoren α^{ten} und β^{ten} Grades ist, so ergibt sich aus den erwähnten Sätzen die Gleichung:

$$\begin{aligned} D(f(x)) = R(f(x),\ f'(x)) &= R(h(x)\,k(x),\ h(x)\,k'(x) + k(x)\,h'(x)) \\ &= R(h(x),\ h(x)\,k'(x) + k(x)\,h'(x)) \cdot R(k(x),\ h(x)\,k'(x) + k(x)\,h'(x)) \\ &= R(h(x),\ k(x)\,h'(x)) \cdot R(k(x),\ h(x)\,k'(x)) \\ &= R(h(x),\ h'(x)) \cdot R(k(x),\ k'(x)) \cdot R(h(x),\ k(x)) \cdot R(k(x),\ h(x)), \end{aligned}$$

es gilt also die wichtige Gleichung:

$$(7)\quad D(h(x) \cdot k(x)) = (-1)^{\alpha\beta}\, D(h(x))\, D(k(x))\, R^2(h(x),\ k(x)).$$

Ist speziell:

$$f(x) = A_0(x - \xi_1) \cdots (x - \xi_n)$$

eine Funktion, welche in lauter Linearfaktoren zerfällt, so folgt aus der Gleichung (5) a. S. 59:

$$(8)\qquad \begin{aligned} D(f(x)) &= R(f(x), f'(x)) = A_0^{\mu-1} f'(\xi_1)\, f'(\xi_2) \cdots f'(\xi_\mu) \\ &= A_0^{2\mu-1}(\xi_1-\xi_2)(\xi_1-\xi_3)\cdots(\xi_\mu-\xi_{\mu-1}), \end{aligned}$$

oder, wenn man die nur durch ihr Vorzeichen sich unterscheidenden Faktoren zusammenfaßt:

$$(8\text{a})\qquad D(f(x)) = (-1)^{\frac{\mu(\mu-1)}{2}} \cdot A_0^{2\mu-1}(\xi_1-\xi_2)^2(\xi_1-\xi_3)^2\cdots(\xi_{\mu-1}-\xi_\mu)^2;$$

hier erkennt man ohne weiteres, daß $D(f(x))$ dann und nur dann verschwindet, wenn mindestens zwei unter den μ Wurzeln $\xi_1, \ldots \xi_\mu$ einander gleich sind. Unter dieser Voraussetzung wird auch die Richtigkeit der Gleichung (7) fast evident; jedoch werde der Beweis dafür dem Leser überlassen.

Viertes Kapitel.

Die Zerlegung der ganzen Funktionen mit p-adischen Koeffizienten in ihre irreduktiblen Faktoren.

---

§ 1. Beweis eines Hilfssatzes.

Die Determinantendarstellung der Resultante $R(f, g)$ benutze ich jetzt zum Beweise eines Satzes, welcher für die folgenden Untersuchungen von fundamentaler Bedeutung ist.

Es seien wieder:

$$(1) \qquad \begin{aligned} f(x) &= A_0 x^\mu + A_1 x^{\mu-1} + \cdots + A_\mu, \\ g(x) &= B_0 x^\nu + B_1 x^{\nu-1} + \cdots + B_\nu \end{aligned}$$

zwei teilerfremde ganze Funktionen μ^{ten} und ν^{ten} Grades von x mit ganzzahligen p-adischen Koeffizienten; dann ist ihre Resultante:

$$(2) \qquad R(f, g) = p^\varrho E$$

eine von Null verschiedene ganze p-adische Zahl, deren Ordnungszahl ϱ sein möge.

Es sei nun:

$$(3) \qquad F(x) = F_0 x^{\mu+\nu-1} + F_1 x^{\mu+\nu-2} + \cdots + F_{\mu+\nu-1}$$

eine beliebige Funktion mit ganzzahligen p-adischen Koeffizienten. Dann kann man stets und zwar auf eine einzige Weise zwei Multiplikatoren:

$$\begin{aligned} f_1(x) &= C_0 x^{\mu-1} + C_1 x^{\mu-2} + \cdots + C_{\mu-1}, \\ g_1(x) &= D_0 x^{\nu-1} + D_1 x^{\nu-2} + \cdots + D_{\nu-1} \end{aligned}$$

bzw. vom $(\mu-1)^{\text{ten}}$ und $(\nu-1)^{\text{ten}}$ Grade mit p-adischen Koeffizienten so bestimmen, daß

$$(4) \qquad f(x)\, g_1(x) + g(x)\, f_1(x) = F(x)$$

ist. Multipliziert man nämlich die linke Seite aus, und setzt dann die Koeffizienten von $x^{\mu+\nu-1}, x^{\mu+\nu-2}, \ldots x, 1$ auf beiden Seiten gleich, so erhält man genau, wie a. S. 55, die $\mu + \nu$ Gleichungen:

$$\begin{array}{llll} (4\text{a}) & A_0 D_0 & + B_0 C_0 & = F_0, \\ & A_1 D_0 + A_0 D_1 & + B_1 C_0 + B_0 C_1 & = F_1, \\ & \dots & & \end{array}$$

deren Determinante eben die Resultante $R(f, g)$, also von Null verschieden ist. Wie also auch die Koeffizienten F_i von $F(x)$ gewählt sein mögen, immer kann man diese Funktion auf eine einzige Weise in der Form (4) darstellen.

Aus den linearen Gleichungen (4a) bestimmen sich die Koeffizienten C_i und D_k als Brüche, deren gemeinsamer Nenner die Resultante $R(f, g) = p^\varrho E$, und deren Zähler eine homogene lineare Funktion von $F_0, F_1, \dots F_{\mu+\nu-1}$ mit ganzzahligen Koeffizienten ist. Besitzt also $F(x)$ den Zahlenteiler p^r, ist also:

$$F(x) = p^r F_0(x),$$

wo $F_0(x)$ eine primitive Funktion ist, so sind alle Koeffizienten F_i durch p^r teilbar. Daher sind alle Koeffizienten C_i und D_k mindestens durch $p^{r-\varrho}$ teilbar, d. h. die Multiplikatoren $f_1(x)$ und $g_1(x)$ haben mindestens den Zahlenteiler $p^{r-\varrho}$. Ist also $r \geqq \varrho$, so besitzen die Multiplikatoren $f_1(x)$ und $g_1(x)$ sicher ebenfalls ganzzahlige p-adische Koeffizienten. So ergibt sich der folgende wichtige Satz:

Sind $f(x)$ und $g(x)$ zwei ganze ganzzahlige teilerfremde Funktionen vom μ^{ten} und ν^{ten} Grade, deren Eliminationsresultante die Ordnungszahl ϱ besitzt, so kann man jede Funktion

(3) $$F(x) = p^r F_0(x),$$

deren Grad kleiner als $\mu + \nu$, und deren Zahlenteiler p^r gleich oder größer als p^ϱ ist, auf eine einzige Weise in der Form:

(4) $$F(x) = f(x)\, g_1(x) + g(x)\, f_1(x)$$

so darstellen, daß die Grade der Multiplikatoren $f_1(x)$ und $g_1(x)$ bzw. kleiner als μ und ν, und daß ihre Zahlenteiler mindestens gleich $p^{r-\varrho}$ sind.

§ 2. Die primären und die irreduktiblen Funktionen mit p-adischen Koeffizienten.

Auf dem im vorigen Abschnitte bewiesenen Hilfssatze beruht nun die Möglichkeit, die ganzen Funktionen von x in ihre einfachsten Bestandteile, die irreduktibeln p-adischen Faktoren zu zerlegen. Wir nennen, entsprechend den Definitionen der gewöhnlichen Algebra, eine Funktion $f(x)$ unzerlegbar oder irreduktibel im

Bereiche der p-adischen Zahlen, wenn sie nicht in Faktoren niedrigeren Grades mit p-adischen Koeffizienten zerlegt werden kann. So sind z. B. offenbar alle Linearfaktoren $Ax - B$ irreduktibel. Dagegen ist die quadratische Funktion $x^2 - A$ nur dann irreduktibel für den Bereich von p, wenn sich innerhalb desselben die Quadratwurzel aus A nicht ausziehen läßt. So ist z. B.

$$x^2 + 1 = (x - 2,1\,2\,1\cdots)(x - 3,3\,2\,3\cdots) \qquad (5)$$

innerhalb $K(5)$ zerlegbar, dagegen $x^2 - 2$ in demselben Bereiche unzerlegbar. Ferner ist:

$$x^3 - 2 = (x - 3,0\,2\,2\,1\cdots)(x^2 + 3,0\,2\,2\,1\cdots x + 4,1\,2\,4\,0\cdots) \qquad (5)$$

innerhalb $K(5)$ zerlegbar, während die auf der rechten Seite auftretende Funktion zweiten Grades für diesen Bereich irreduktibel ist. Aus den angeführten Beispielen geht hervor, daß eine für den Bereich $K(1, x)$ irreduktible Funktion innerhalb des Bereiches der p-adischen Zahlen noch in Faktoren niedrigeren Grades zerfallen kann; denn es fällt ja hier die Beschränkung weg, daß die Koeffizienten rationale, d. h. periodische p-adische Zahlen sein sollen. Unser Begriff der Irreduktibilität ist also enger als der gewöhnliche.

Zunächst ist eine irreduktible Funktion nur bis auf einen multiplikativen Zahlenfaktor bestimmt. Wir wollen auch diesen Zahlenfaktor für alle reduktiblen und irreduktiblen Funktionen ein für allemal dadurch fixieren, daß wir eine bestimmte unter diesen verschiedenen Funktionen als **primär** bezeichnen:

Eine Funktion:

$$(1) \qquad F(x) = p^{\alpha} x^m + A_1 x^{m-1} + \cdots + A_m$$

soll primär heißen, wenn sie primitiv ist, und wenn zugleich der Koeffizient der höchsten Potenz $A_0 = p^{\alpha}$ eine reine Potenz von p ist.

Jede Funktion $F(x)$ läßt sich dann offenbar auf eine einzige Weise in der Form:

$$(1\text{a}) \qquad F(x) = A \cdot F_0(x)$$

darstellen, wo $A = p^{\delta} \cdot E$ ein Zahlenfaktor und $F_0(x)$ eine primäre Funktion ist. Das Produkt

$$F_0(x)\,G_0(x) = (p^{\alpha} x^m + \cdots)(p^{\beta} x^n \cdots) = p^{\alpha+\beta} x^{m+n} + \cdots$$

zweier primären Funktionen ist wieder primär, da dasselbe ebenfalls keinen Zahlenteiler hat. Zerfällt endlich eine primäre Funktion $F_0(x)$ in ein Produkt zweier Faktoren niedrigeren Grades, ist also:

$$(2) \qquad F_0(x) = f(x)\,g(x)$$

so ist dieselbe Funktion auch gleich dem Produkte zweier primärer Faktoren derselben Grade. In der Tat, sei $f(x)$ noch nicht primär, und es sei $f(x) = af_0(x)$, wo $f_0(x)$ primär ist. Schreibt man dann (2) in der Form:

$$F_0(x) = f_0(x)\,(ag(x)) = f_0(x)\,g_0(x),$$

so muß $ag(x) = g_0(x)$ auch primär sein, denn einmal hat $g_0(x)$ keinen Zahlenteiler, weil sonst das Produkt $f_0(x)\,g_0(x)$ denselben Zahlenteiler haben würde und zweitens folgt durch Koeffizientenvergleichung aus der Gleichung:

$$(p^\alpha x^n + \cdots) = (p^\beta x^\mu + \cdots)\,(g_0 x^\nu + g_1 x^{\nu-1} + \cdots),$$

daß der Koeffizient $g_0 = p^\gamma$ eine reine Potenz von p sein muß.

Ist speziell $p^\alpha = 1$, so folgt durch Koeffizientenvergleichung, daß auch $p^\beta = p^\gamma = 1$ sein muß; ist dagegen $p^\alpha > 1$, so muß mindestens eine der beiden Potenzen p^β und p^γ noch größer als Eins sein.

Es gelten nun für die irreduktibeln Funktionen $P(x)$ mit p-adischen Koeffizienten dieselben Sätze wie für diejenigen mit rationalen Koeffizienten und zwar wollen wir die folgenden herleiten:

I) Eine irreduktible p-adische Funktion $P(x)$ ist in einer andern Funktion $F(x)$ entweder als Teiler enthalten oder sie ist zu ihr teilerfremd.

Hätten nämlich $P(x)$ und $F(x)$ einen gemeinsamen Teiler, so könnte man ihren größten gemeinsamen Teiler $D(x)$ durch das Euklidische Verfahren rational bestimmen, und $D(x)$ wäre ebenfalls eine ganze Funktion mit p-adischen Koeffizienten. Dann wäre aber gegen unsere Voraussetzung $P(x) = D(x)\,\overline{P}(x)$ als Produkt zweier Funktionen von niedrigerem Grade dargestellt.

II) Eine irreduktible Funktion ist in dem Produkte zweier oder mehrerer Funktionen nur dann enthalten, wenn sie in einem jener Faktoren aufgeht.

Denn wenn $f(x) \cdot f_1(x)$ den Teiler $P(x)$ enthält, $f(x)$ aber nicht, so sind $f(x)$ und $P(x)$ teilerfremd; also kann man die ganzen Funktionen $\bar{f}(x)$ und $\overline{P}(x)$ so bestimmen, daß:

$$f(x)\,\bar{f}(x) + P(x)\,\overline{P}(x) = 1 \qquad (p)$$

ist. Multipliziert man diese Gleichung mit $f_1(x)$, so folgt:

$$(f(x) \cdot f_1(x))\,\bar{f}(x) + P(x)\,f_1(x)\,\overline{P}(x) = f_1(x) \qquad (p),$$

und hier ist die linke Seite nach Voraussetzung durch $P(x)$ teilbar, also muß auch $f_1(x)$ ein Vielfaches von $P(x)$ sein.

III) Zwei Produkte irreduktibler Funktionen sind nur dann gleich, wenn sie identisch sind.

Ist nämlich

$$A P_1(x) P_2(x) \cdots P_k(x) = B Q_1(x) Q_2(x) \cdots Q_k(x) \qquad (p),$$

wo A und B Zahlen und die $P_i(x)$ und $Q_i(x)$ irreduktible Funktionen sind, so muß z. B. die Funktion $P_1(x)$ abgesehen von einem Zahlenfaktor mit einem der Faktoren $Q_i(x)$ identisch sein, weil sie ein Teiler des rechts stehenden Produktes ist. Ist aber z. B. $P_1(x)$ gleich $Q_1(x)$, so kann man die obige Gleichung durch $P_1(x)$ dividieren und dann für $P_2(x)$ in gleicher Weise weiter schließen usw. Zuletzt ergibt sich dann $A = B$ und damit der vollständige Beweis unserer Behauptung.

§ 3. Die Zerlegung der ganzen Funktionen mit p-adischen Koeffizienten in ihre irreduktiblen Faktoren.

Ich beweise jetzt den für die ganze Theorie grundlegenden Satz:

IV) Eine Funktion $F(x)$ mit p-adischen Koeffizienten ist auf eine und nur eine Weise in irreduktible p-adische Faktoren zerlegbar, und es gibt ein endliches Verfahren, um diese Faktoren mit jeder vorgegebenen Genauigkeit zu berechnen.

Ist die Zerlegbarkeit einmal bewiesen, so folgt aus Satz III), daß die Zerlegung in irreduktible Faktoren nur auf eine Weise möglich ist. Ferner brauchen wir nur ein endliches Verfahren anzugeben, mit dessen Hilfe eine beliebige Funktion in zwei Faktoren niedrigeren Grades zerlegt oder bewiesen werden kann, daß eine solche Zerlegung nicht möglich ist. Ist nämlich

$$F(x) = f(x) \cdot g(x) \quad (p), \tag{1}$$

so kann ja jeder Faktor für sich weiter untersucht und in derselben Weise solange fortgefahren werden, bis eine weitere Zerlegung nicht mehr möglich ist.

Der Einfachheit wegen wollen und können wir die ganzzahlige Funktion $F(x)$ als primär annehmen; es sei also

$$F(x) = p^{\alpha_0} x^n + A_1 x^{n-1} + \cdots + A_n. \tag{2}$$

Ist dann eine Zerlegung (1) überhaupt möglich, so kann man nach dem a. S. 65 bewiesenen Satz die beiden Funktionen $f(x)$ und $g(x)$ ebenfalls als primär annehmen, sie werden also die Form haben

$$\begin{aligned} f(x) &= p^{\beta_0} x^{\mu} + B_1 x^{\mu-1} + \cdots + B_{\mu}, \\ g(x) &= p^{\gamma_0} x^{\nu} + C_1 x^{\nu-1} + \cdots + C_{\nu}. \end{aligned} \tag{3}$$

Besteht nun für $F(x)$ eine Zerlegung (1), so folgt aus ihr, wenn wir zu den Näherungswerten übergehen, für ein beliebig großes k die Kongruenz

$$F^{(k)}(x) \equiv f^{(k)}(x) \cdot g^{(k)}(x) \qquad (\operatorname{mod} p^{k+1}). \tag{4}$$

Sobald $F(x)$ in zwei Faktoren μ^{ten} und ν^{ten} Grades zerfällt, besteht also für jeden ihrer Näherungswerte $F^{(k)}(x)$ eine analoge Zerlegung. Wir haben daher zunächst das Resultat, daß eine Zerlegung der primären Funktion $F(x)$ in zwei Faktoren μ^{ten} und ν^{ten} Grades nur dann möglich ist, wenn jeder ihrer Näherungswerte $F^{(k)}(x)$ modulo p^{k+1} in zwei ganzzahlige primäre Faktoren der gleichen Grade zerfällt.

Die Frage, ob eine ganzzahlige Funktion $F^{(k)}(x)$ für den Modul p^{k+1} überhaupt in zwei Faktoren zerfällt oder nicht, kann für jeden Wert von k durch eine endliche Anzahl von Versuchen entschieden werden. Man braucht ja nur alle modulo p^{k+1} inkongruenten ganzen ganzzahligen Funktionen vom $(n-1)^{\text{ten}}$ und von niedrigerem Grade, deren Anzahl immer endlich ist, hinzuschreiben, und je zwei unter ihnen, deren Grade sich zu n ergänzen, miteinander zu multiplizieren. Ist dann eins jener Produkte kongruent $F^{(k)}(x)$ modulo p^{k+1}, so ist $F^{(k)}(x)$ für diesen Modul zerlegbar. Im entgegengesetzten Falle ist $F^{(k)}(x)$ unzerlegbar, und daraus folgt dann sofort, daß auch $F(x)$ nicht in zwei ganzzahlige Faktoren niedrigeren Grades mit p-adischen Koeffizienten zerlegt werden kann. Dagegen folgt aus der Zerlegbarkeit der Näherungsfunktion $F^{(k)}(x)$ modulo p^{k+1} bis jetzt noch keineswegs die Zerlegbarkeit von $F(x)$ selbst. Durch die folgenden Betrachtungen wird aber die letzte Aufgabe vollständig auf die Lösung der ersten zurückgeführt.

Wir wollen voraussetzen, daß die Diskriminante $D(F)$ von $F(x)$ von Null verschieden ist. Hierin liegt keine Beschränkung: denn wenn $D(F) = 0$ ist, so hat die Funktion $F(x)$ mit ihrer ersten Ableitung $F'(x)$ einen gemeinsamen Teiler $D(x)$, den wir durch das Euklidische Verfahren bestimmen können. Wir hätten damit also sofort eine Zerlegung von $F(x)$ in zwei Faktoren niedrigeren Grades gewonnen. Es sei also

$$D(F) = p^{\delta} E, \tag{5}$$

wo die Ordnungszahl δ eine ganze nicht negative Zahl ist, welche, wie beiläufig bemerkt werde, gleich oder größer als α_0 sein muß. Denn aus der a. S. 56 gegebenen Darstellung (7) von $D(F)$ in Determinantenform folgt ja, daß $D(F)$ durch $A_0 = p^{\alpha_0}$ teilbar ist, weil die beiden einzigen in der ersten Kolonne stehenden von Null verschiedenen Elemente Multipla von A_0 sind.

Ist nun $F^{(r)}(x)$ ein Näherungswert von $F(x)$, dessen Index $r \geqq \delta$ ist, so ist:

$$D(F^{(r)}) \equiv D(F) \pmod{p^{r+1}}, \tag{4a}$$

d. h. auch die Diskriminante von $F^{(r)}(x)$ besitzt genau die Ordnung δ.

Die Frage nach der Zerlegbarkeit von $F(x)$ wird nun völlig entschieden durch den folgenden wichtigen Satz:

Ist die Diskriminante von $F(x)$ von der Ordnung δ, so zerfällt die Funktion $F(x)$ dann und nur dann in Faktoren niedrigeren Grades, wenn ihr δ^{ter} Näherungswert $F^{(\delta)}(x)$ modulo $p^{\delta+1}$ zerfällt, und zwar entspricht jeder Zerlegung

$$F^{(\delta)}(x) \equiv \bar{f}(x)\,\bar{g}(x) \pmod{p^{\delta+1}}$$

eine eindeutig bestimmte Zerlegung von $F(x)$ in p-adische Faktoren

$$F(x) = f(x)\,g(x) \quad (p)$$

in der Weise, daß $\bar{f}(x)$ und $\bar{g}(x)$ Näherungswerte von $f(x)$ und $g(x)$ sind.

Um diesen Beweis allgemein zu führen, nehme ich an, wir kennen schon eine Zerlegung

$$(6) \qquad F^{(r)}(x) \equiv f_0(x)\,g_0(x) \pmod{p^{r+1}}$$

irgend eines Näherungswertes von $F(x)$ in zwei Faktoren μ^{ten} und ν^{ten} Grades für einen Index r, welcher größer oder gleich δ ist; dann zeige ich, daß und wie man zwei Zusatzfunktionen $f_1(x)$ und $g_1(x)$ von niedrigerem als dem μ^{ten} und ν^{ten} Grade so bestimmen kann, daß auch für den nächsthöheren Näherungswert $F^{(r+1)}(x)$ die entsprechende Kongruenz:

$$(6\text{a}) \qquad F^{(r+1)}(x) \equiv (f_0(x) + f_1(x))\,(g_0(x) + g_1(x)) \pmod{p^{r+2}}$$

besteht. Hierbei bestimmen sich, wie gleich bewiesen wird, die Zusatzfunktionen $f_1(x)$ und $g_1(x)$ von selbst so, daß ihre Zahlenteiler mindestens gleich $p^{r+1-\delta}$ sind, d. h. daß:

$$f_1(x) = p^{r+1-\delta}\,\mathfrak{f}_1(x), \qquad g_1(x) = p^{r+1-\delta}\,\mathfrak{g}_1(x)$$

ist. Wendet man nun dasselbe Verfahren der Reihe nach für $r = \delta$, $\delta + 1$, $\delta + 2 \cdots$ an, so erhält man zuletzt mit jeder vorgegebenen Genauigkeit zwei wohldefinierte Funktionen μ^{ten} und ν^{ten} Grades:

$$\begin{aligned} f(x) &= \mathfrak{f}_0(x) + p\,\mathfrak{f}_1(x) + p^2\,\mathfrak{f}_2(x) + \cdots \\ g(x) &= \mathfrak{g}_0(x) + p\,\mathfrak{g}_1(x) + p^2\,\mathfrak{g}_2(x) + \cdots \end{aligned} \quad (p)$$

des Bereiches $K(p, x)$, für welche die Gleichung:

$$F(x) = f(x) \cdot g(x) \quad (p)$$

besteht; und damit ist unsere Aufgabe dann vollständig gelöst.

Zum Beweise, daß aus der Kongruenz (6) die Kongruenz (6a) hergeleitet werden kann, schreibe ich die letztere in der Form:

$$(6\text{b}) \quad \begin{aligned} F^{(r+1)}(x) - f_0(x)\,g_0(x) &= (F^{(r+1)}(x) - F^{(r)}(x)) + (F^{(r)}(x) - f_0(x)\,g_0(x)) \\ &\equiv f_0(x)\,g_1(x) + f_1(x)\,g_0(x) + f_1(x)\,g_1(x) \pmod{p^{r+2}}. \end{aligned}$$

Dann ist die linke Seite eine gegebene ganze ganzzahlige Funktion von niedrigerem als dem $n = (\mu + \nu)^{\text{ten}}$ Grade, da sich die Glieder n^{ter} Ordnung, welche alle gleich $\pm p^{\alpha_0} x^n$ sind, wegheben, und sie besitzt den Zahlenteiler p^{r+1}, da dies sowohl für $F^{(r+1)}(x) - F^{(r)}(x)$ als für $F^{(r)}(x) - f_0(x) g_0(x)$ der Fall ist; das erste folgt ja aus der Definition der Näherungswerte, das zweite aus der vorausgesetzten Kongruenz (6). Setzen wir diese bekannte Funktion gleich $p^{r+1}\mathfrak{F}_0(x)$, so haben wir also

$$f_1(x) = p^{r+1-\delta}\mathfrak{f}_1(x), \qquad g_1(x) = p^{r+1-\delta}\mathfrak{g}_1(x)$$

so zu bestimmen, daß:

$$p^{r+1-\delta}(f_0(x)\mathfrak{g}_1(x) + g_0(x)\mathfrak{f}_1(x)) + p^{2r+2-2\delta}\mathfrak{f}_1(x)\mathfrak{g}_1(x) \equiv p^{r+1}\mathfrak{F}_0(x) \pmod{p^{r+2}}$$

wird, oder nach Division mit $p^{r+1-\delta}$:

(6c) $f_0(x)\mathfrak{g}_1(x) + g_0(x)\mathfrak{f}_1(x) + p^{r+1-\delta}\mathfrak{f}_1(x)\mathfrak{g}_1(x) \equiv p^{\delta}\mathfrak{F}_0(x) \pmod{p^{\delta+1}}$.

Diese Aufgabe kann aber immer gelöst werden. Es sei nämlich ϱ die Ordnungszahl der Eliminationsresultante $R(f_0, g_0)$ von f_0 und g_0, so folgt aus der a. S. 60 bewiesenen Gleichung (7):

$$D(f_0 \cdot g_0) = \pm D(f_0) D(g_0) R^2(f_0, g_0)$$

und der Kongruenz (6) die neue Kongruenz:

$$D(F^{(r)}(x)) \equiv \pm D(f_0) D(g_0) R^2(f_0, g_0) \pmod{p^{r+1}}.$$

Da die Diskriminanten $D(f_0)$ und $D(g_0)$ von $f_0(x)$ und $g_0(x)$ Zahlen von nicht negativer Ordnung sind, so ergibt sich hieraus, daß die Ordnungszahl 2ϱ von $R^2(f_0, g_0)$ höchstens gleich der Ordnungszahl δ von $D(F^{(r)})$ ist, d. h. daß

(7) $$\varrho \leqq \frac{\delta}{2}$$

sein muß.

Folglich ist die in der Kongruenz (6c) rechtsstehende Funktion $p^{\delta}\mathfrak{F}_0(x)$ von niedrigerem als dem $(\mu + \nu)^{\text{ten}}$ Grade und ihr Zahlenteiler größer als p^{ϱ}. In diesem Falle kann man aber nach dem auf Seite 63 bewiesenen Hilfssatze zwei Multiplikatoren $\bar{\mathfrak{f}}_1(x)$ und $\bar{\mathfrak{g}}_1(x)$, deren Grad bzw. höchstens gleich $(\mu - 1)$ und $(\nu - 1)$ und deren Zahlenteiler mindestens gleich $p^{\delta-\varrho}$ ist, so bestimmen, daß für den Bereich von p:

$$f_0(x)\bar{\mathfrak{g}}_1(x) + g_0(x)\bar{\mathfrak{f}}_1(x) = p^{\delta}\mathfrak{F}_0(x) \quad (p)$$

ist. Betrachtet man diese Gleichung als Kongruenz für den Modul $p^{\delta+1}$ und bezeichnet man die δ^{ten} Näherungswerte von $\bar{\mathfrak{f}}_1(x)$ und $\bar{\mathfrak{g}}_1(x)$ bzw. durch $\mathfrak{f}_1(x)$ und $\mathfrak{g}_1(x)$, so haben auch sie mindestens den Zahlenteiler $p^{\delta-\varrho}$ *) und es besteht für sie die Kongruenz:

$$f_0(x)\mathfrak{g}_1(x) + g_0(x)\mathfrak{f}_1(x) \equiv p^{\delta}\mathfrak{F}_0(x) \pmod{p^{\delta+1}}.$$

*) Also erhalten die Zusatzfunktionen $f_1(x)$ und $g_1(x)$ in (6a) mindestens den Zahlenteiler $p^{r+1-\delta} \cdot p^{\delta-\varrho} = p^{r+1-\varrho}$, und $f_0(x)$ ist somit ein Näherungswert $(r-\varrho)^{\text{ter}}$ Ordnung von $f(x) = f_0(x) + f_1(x) + \cdots$.

Dieselben Funktionen befriedigen aber auch die Bedingungskongruenz (6c), denn $\mathfrak{f}_1(x)$ und $\mathfrak{g}_1(x)$ sind ja mindestens durch $p^{\delta-\varrho}$ und somit das links noch auftretende Glied $p^{r+1-\delta}\mathfrak{f}_1(x)\,\mathfrak{g}_1(x)$ mindestens durch $p^{r+1+\delta-2\varrho}$ teilbar. Da nun nach (7) $\delta-2\varrho\geqq 0$, und nach Voraussetzung $r\geqq\delta$ ist, so ist jenes Zusatzglied mindestens durch $p^{\delta+1}$ teilbar und kann daher weggelassen werden.

Hiermit ist die Aufgabe, eine beliebige Funktion n^{ten} Grades in irreduktible p-adische Faktoren zu zerlegen, vollständig gelöst, und es ist leicht, eine solche Zerlegung wirklich durchzuführen. Zu diesem Zwecke bestimme man zunächst die in der Diskriminante der vorgelegten Funktion $F(x)$ enthaltene Potenz p^{δ} von p und untersuche, ob der δ^{te} Näherungswert $F^{(\delta)}(x)$ von $F(x)$ für den Modul $p^{\delta+1}$ Teiler besitzt oder nicht. Besitzt er keine Teiler, so ist $F(x)$ für den Bereich von p irreduktibel. Ist dagegen $F^{(\delta)}(x)$ zerlegbar für den Modul $p^{\delta+1}$ und ist $P_1{}^0(x)$ der oder wenigstens ein Teiler vom niedrigsten Grade, so folgt aus der Kongruenz:

$$F^{(\delta)}(x)\equiv P_1{}^0(x)\,F_1{}^0(x)\pmod{p^{\delta+1}}$$

nach dem soeben bewiesenen Satze, daß $F(x)$ einen Teiler $P_1(x)$ hat, dessen Näherungswert $P_1{}^0(x)$ ist, d. h. es ergiebt sich eine Gleichung:

(8) $$F(x)=P_1(x)\,F_1(x)\quad(p).$$

Der so bestimmte Faktor $P_1(x)$ ist nun in der Tat eine Primfunktion. Denn zerfiele etwa $P_1(x)$ in das Produkt $p_1(x)\,p_2(x)$ zweier Faktoren niedrigeren Grades, so wäre nach dem Vorigen auch $P_1{}^0(x)$ zerlegbar; da dies nach Voraussetzung nicht der Fall ist, so muß $P_1(x)$ eine Primfunktion sein. Ferner ist $P_1(x)$ ein Primfaktor niedrigsten Grades von $F(x)$, denn sonst würde ja auch $F^{(\delta)}(x)$ modulo $p^{\delta+1}$ einen Faktor niedrigeren Grades haben. Wendet man dasselbe Verfahren auf $F_1(x)$ in (8) an und fährt so fort, so erhält man schließlich die vollständige Zerlegung von $F(x)$ in Primfaktoren:

$$F(x)=P_1(x)\,P_2(x)\ldots P_\lambda(x)\quad(p),$$

wo die Funktionen $P_i(x)$ nach steigenden Graden geordnet sind. Die Eindeutigkeit dieser Zerlegung abgesehen von Zahlenfaktoren ist schon früher in III a. S. 65 bewiesen worden.

§ 4. Folgerungen. Einfachere Kriterien für die Zerlegbarkeit der ganzen Funktionen. Die Eisensteinschen Funktionen.

Nach dem im vorigen Abschnitt bewiesenen Fundamentalsatz ist die Aufgabe, eine Funktion $F(x)$ mit p-adischen Koeffizienten in ihre irreduktiblen p-adischen Faktoren zu zerlegen, theoretisch vollkommen gelöst. Ist aber die Ordnungszahl δ der Diskriminante $D(f)$ etwas

groß, so ist die Zerlegung von $f(x)$ modulo $p^{\delta+1}$ nicht immer leicht zu bewerkstelligen. Aus diesem Grunde sollen noch einige für das Folgende wichtige Fälle behandelt werden, in denen diese Frage entweder einfacher gelöst werden, oder in denen die Irreduktibilität der Funktion $f(x)$ direkt erkannt werden kann.

Zunächst folgt aus den Betrachtungen des vorigen Paragraphen sofort der Satz:

Weiß man, daß für die Funktion $F(x)$ eine Kongruenz

(1) $$F(x) \equiv f_0(x)\, g_0(x) \pmod{p^{r+1}}$$

für eine Potenz von p als Modul besteht, deren Exponent $(r+1)$ größer ist als die Ordnungszahl 2ϱ des Quadrates $R^2(f_0(x), g_0(x))$ der Eliminationsresultante jener beiden Faktoren, so besteht auch für $F(x)$ eine Zerlegung:

(1a) $$F(x) = f(x)\, g(x) \quad (p)$$

in zwei p-adische Faktoren desselben Grades, deren $(r-\varrho)^{\text{te}}$ Näherungswerte bzw. $f_0(x)$ und $g_0(x)$ sind.

In der Tat erhalten ja die Zusatzfunktionen $f_1(x)$ und $g_1(x)$ in (6a) a. S. 68 bei der dort durchgeführten Bestimmung nach S. 69 Anm. mindestens den Zahlenteiler $p^{r+1-\varrho}$. Bei der hier gemachten Annahme $r+1 > 2\varrho$ erfüllen sie also genau wie vorher jene Kongruenz (6a), da ihr Produkt $f_1(x)\, g_1(x)$ wieder modulo p^{r+2} fortgelassen werden kann.

Die wichtigste Anwendung dieses Satzes ergibt sich, wenn man den einen der beiden Faktoren $f(x) = x - \xi$ als linear voraussetzt, wenn man also untersucht, unter welcher Bedingung eine vorgelegte Funktion $F(x)$ einen p-adischen Linearfaktor $x - \xi$ hat, oder, was dasselbe ist, wann eine gegebene Gleichung:

(2) $$F(x) = 0 \quad (p)$$

eine p-adische Wurzel $x = \xi$ besitzt. Die Antwort auf diese Frage wird durch den folgenden Satz gegeben:

Kann man eine ganze positive Zahl ξ_0 so bestimmen, daß der Quotient

(3) $$\frac{F(\xi_0)}{(F'(\xi_0))^2}$$

von positiver Ordnung ist, so besitzt die Gleichung $F(x) = 0$ eine p-adische Wurzel $x = \xi$, deren Näherungswert gleich ξ_0 ist, und mit jeder vorgegebenen Genauigkeit berechnet werden kann.

In der Tat, sei $F(\xi_0)$ genau durch p^{r+1} teilbar, dann besteht für ein variables x die Kongruenz:

(4) $$F(x) \equiv F(x) - F(\xi_0) \equiv (x - \xi_0)\, g_0(x) \pmod{p^{r+1}},$$

d. h. $F(x)$ zerfällt modulo p^{r+1} in das Produkt aus einem Linearfaktor und dem anderen Faktor $g_0(x)$. Ist also p^{r+1} oder $F(\xi_0)$ von höherer Ordnung als

$$R^2(x - \xi_0,\ g_0(x)) = g_0(\xi_0)^2, \tag{5}$$

so entspricht nach dem soeben bewiesenen allgemeinen Satze der obigen Zerlegung modulo p^{r+1} eine andere

$$F(x) = (x - \xi)\, g(x) \quad (p)$$

in p-adische Faktoren. Dies ist aber der Fall, denn differenziert man die Kongruenz (4) nach x und setzt dann $x = \xi_0$, so ergibt sich

$$F'(\xi_0) \equiv g_0(\xi_0) \equiv R(x - \xi_0,\ g_0(x)) \pmod{p^{r+1}},$$

und da n. d. V. $F'(\xi_0)^2$ also auch $R^2(x - \xi_0,\ g_0(x))$ von niedrigerer als der $(r+1)^{\text{ten}}$ Ordnung ist, so ist unsere Behauptung vollständig bewiesen.

So brauchbar dieser Satz in den meisten Fällen auch ist, so wollen wir ihn doch noch durch einen wesentlich schärferen ersetzen, der jetzt sehr einfach abgeleitet werden kann. Die aus ihm sich ergebende angenäherte Berechnung der p-adischen Gleichungswurzeln ist nichts anderes als die bekannte Newtonsche Approximationsmethode, übertragen auf die p-adischen Zahlen. Es sei ξ_0 eine p-adische Zahl, welche die gegebene Gleichung ν^{ten} Grades $F(x) = 0$ näherungsweise befriedigt, und zwar sei $F(\xi_0)$ von der ϱ^{ten} Ordnung, also:

$$F(\xi_0) = a_\varrho p^\varrho + a_{\varrho+1} p^{\varrho+1} + \cdots .$$

Wir stellen uns die Aufgabe, die p-adische Zahl h so zu bestimmen, daß $\xi_0 + h$ ein genauerer Näherungswert der Wurzel wird, daß also die Ordnungszahl von

$$F(\xi_0 + h) = F(\xi_0) + F'(\xi_0)\, h + \frac{F''(\xi_0)}{2!} h^2 + \cdots + \frac{F^{(\nu)}(\xi_0)}{\nu!} h^\nu \tag{6}$$

größer als ϱ, d. h. mindestens gleich $\varrho + 1$ ist. Es seien nun die Ordnungszahlen von

$$F(\xi_0), \quad F'(\xi_0), \quad \frac{F''(\xi_0)}{2!}, \ldots \frac{F^{(\nu)}(\xi_0)}{\nu!}$$

bzw. gleich

$$\varrho, \quad \varrho', \quad \varrho'', \quad \ldots \varrho^{(\nu)}.$$

Ist dann der Näherungswert ξ_0 genügend genau, also die Ordnungszahl ϱ von $F(\xi_0)$ so groß, daß das Korrektionsglied h schon von hoher Ordnungszahl ist, so wird man einen besseren Näherungswert erhalten, wenn man in der Gleichung (6) die mit $h^2, \ldots h^\nu$ multiplizierten Glieder fortläßt und das Zusatzglied h aus der linearen Gleichung

$$F(\xi_0) + hF'(\xi_0) = 0, \qquad h = -\frac{F(\xi_0)}{F'(\xi_0)} \qquad (p)$$

berechnet. Diese Bestimmung, welche eben mit der Newtonschen Annäherungsmethode identisch ist, wird hier in der Zahl $\xi_0' = \xi_0 + h$ dann und nur dann einen genaueren Näherungswert liefern, wenn für das so bestimmte h alle Zusatzglieder

$$\frac{F''(\xi_0)}{2!}h^2, \quad \frac{F'''(\xi_0)}{3!}h^3, \ldots, \quad \frac{F^{(\nu)}(\xi_0)}{\nu!}h^\nu$$

von höherer als der ϱ^{ten} Ordnung werden, denn dann wird ja der Koeffizient von p^ϱ in der Entwicklung von $F(\xi_0 + h)$ gleich Null, d. h. $F(\xi_0 + h)$ erhält mindestens die Ordnungszahl $(\varrho + 1)$.

Da nun die Ordnungszahl von $h = -\frac{F(\xi_0)}{F'(\xi_0)}$ gleich $\varrho - \varrho'$, die von $\frac{F^{(i)}(\xi_0)}{i!}$ gleich $\varrho^{(i)}$ ist, so muß ϱ so groß sein, daß allgemein:

$$\varrho^{(i)} + i(\varrho - \varrho') > \varrho \qquad (i = 2, 3, \ldots \nu)$$

$$(7) \qquad \varrho > \frac{i\varrho' - \varrho^{(i)}}{i - 1}$$

ist. Ist also ξ_0 bereits ein so genauer Näherungswert für unsere Gleichungswurzel, daß für die Ordnungszahl ϱ von $F(\xi_0)$

$$(7\text{a}) \qquad \varrho > \text{Max.}\left(\frac{2\varrho' - \varrho''}{1}, \quad \frac{3\varrho' - \varrho'''}{2}, \ldots \frac{\nu\varrho' - \varrho^{(\nu)}}{\nu - 1}\right)$$

ist, so liefert die hier angegebene rationale Bestimmung von h einen genaueren Näherungswert

$$\xi_0' = \xi_0 + h.$$

Ersetzt man nun den Näherungswert ξ_0 durch den genaueren $\xi_0' = \xi_0 + h$, so muß man erst beweisen, daß man aus ihm durch dieselbe Methode eine noch größere Annäherung erhält. Es ist leicht zu zeigen, daß dies immer der Fall ist, wenn ϱ groß genug, d. h. wenn der erste Näherungswert ξ_0 schon genau genug ist. Dies ist aber sicher der Fall, wenn man beweisen kann, daß die Ordnungszahlen $\varrho', \varrho'', \ldots \varrho^{(\nu)}$ ungeändert bleiben, wenn man ξ_0 durch $\xi_0 + h$ ersetzt. Bei der wichtigen Anwendung, welche von dieser Newtonschen Näherungsmethode im achten Kapitel gemacht werden wird, folgt aus der Natur der vorgelegten Gleichung, daß die Ordnungszahlen $\varrho', \varrho'', \ldots \varrho^{(\nu)}$ ungeändert bleiben; für sie ergibt also diese Methode die Bestimmung der Wurzel ξ mit jeder vorgegebenen Genauigkeit. Den so bewiesenen Satz kann man also folgendermaßen aussprechen:

Ist ξ_0 ein solcher Näherungswert der Gleichung ν^{ten} Grades $F(x) = 0$, daß:

$$F(\xi_0) \equiv 0 \pmod{p^\varrho}$$

und

$$\varrho > \operatorname{Max}\left(\frac{i\varrho' - \varrho^{(i)}}{i-1}\right) \qquad (i = 2, 3, \cdots \nu)$$

ist, wo allgemein $\varrho^{(i)}$ die Ordnungszahl von $\frac{F^{(i)}(\xi_0)}{i!}$ ist, so besitzt die obige Gleichung eine p-adische Wurzel, für welche

$$\xi \equiv \xi_0 \pmod{p^{\varrho - \varrho'}}$$

ist, und welche mit jeder vorgegebenen Genauigkeit durch die Newtonsche Näherungsmethode gefunden werden kann, vorausgesetzt, daß die Ordnungszahlen $\varrho', \varrho'', \ldots \varrho^{(\nu)}$ bei den sukzessiven Annäherungen ungeändert bleiben.

Aus dem ersten Satze dieses Paragraphen ziehen wir jetzt noch eine wichtige Folgerung.

Ist

$$F(x) = A_\lambda x^\lambda + A_{\lambda-1}x^{\lambda-1} + \cdots + A_0$$

eine ganzzahlige primitive Funktion, welche irreduktibel ist, und ist einer ihrer äußeren Koeffizienten A_0 oder A_λ durch p teilbar, so müssen auch alle inneren Koeffizienten

$$A_{\lambda-1},\ A_{\lambda-2},\ \ldots A_1$$

p enthalten, so daß dann also der andere äußere Koeffizient allein eine Einheit ist. In einer irreduktiblen primitiven Funktion können also nicht beide äußeren Koeffizienten durch p teilbar sein.

Beim Beweise dieses für das weitere wichtigen Satzes kann und will ich voraussetzen, daß A_0 durch p teilbar ist; enthielte nämlich A_λ diese Primzahl, so könnte ich an Stelle von $F(x)$ die andere Funktion

$$\bar{F}(x) = A_0\bar{x}^\lambda + A_1\bar{x}^{\lambda-1} + \cdots + A_\lambda$$

betrachten, welche offenbar dann und nur dann zerlegbar ist, wenn das gleiche für $F(x)$ gilt.

Ist nun A_0 ein Multiplum von p, und wären, entgegen unserer Behauptung, nicht alle Koeffizienten $A_{\lambda-1}, \ldots A_1$ durch p teilbar, so sei A_μ in dieser Reihe der letzte p nicht enthaltende Koeffizient. Dann besteht also für $F(x)$ die folgende Kongruenz modulo p:

(8) $$F(x) \equiv (A_\lambda x^{\lambda-\mu} + \cdots + A_\mu)x^\mu = \varphi_0(x)x^\mu \pmod{p},$$

d. h. $F(x)$ zerfällt modulo p in zwei Faktoren $(\lambda - \mu)^{\text{ten}}$ und μ^{ten} Grades; die Resultante:

$$R(x^\mu, \varphi(x)) = R((x-0)^\mu, \varphi(x))$$

jener beiden Faktoren ist nicht durch p teilbar, denn nach dem a. S. 59 (4a) bewiesenen Satze ist sie gleich $\varphi(0)^\mu = A_\mu^\mu$. Wendet man also auf die Kongruenz (8) den Satz (1) an, und beachtet, daß hier $2\varrho = 0$, $r + 1 = 1$ ist, so würde aus ihr folgen, daß $F(x)$ in zwei p-adische

Faktoren zerfiele, was unserer Voraussetzung widerspricht; unsere Behauptung ist somit bewiesen.

Derselbe Satz besteht auch, wenn

$$F(x) = A_\lambda x^\lambda + \cdots + A_0$$

die Potenz einer irreduktiblen Funktion ist, also lauter gleiche irreduktible Faktoren besitzt;

denn wäre $A_0 \equiv 0 \pmod p$ und A_μ wieder der letzte p nicht enthaltende Koeffizient, so folgte ja aus der Kongruenz (8) eine Gleichung

$$F(x) = \varphi(x)\psi(x) \quad (p),$$

deren nullten Näherungswerte $\varphi_0(x)$ und x^μ wären, und diese beiden Funktionen sind teilerfremd, da ihre Resultante:

$$R(\psi(x),\ \varphi(x)) \equiv R(x^\mu,\ \varphi_0(x)) \equiv A_\mu^\mu \pmod p$$

durch p nicht teilbar ist; diese Folgerung widerspricht aber der Voraussetzung, daß $F(x)$ lauter gleiche irreduktible Faktoren haben soll.

Es sei nun

$$F(x) = a_0 x^\lambda + p a_1 x^{\lambda-1} + \cdots + p a_\lambda \tag{9}$$

eine primitive Funktion, deren Koeffizienten außer dem ersten a_0 alle durch p teilbar sind. Aus einem gleich anzugebenden Grunde soll eine solche Funktion eine Eisensteinsche Funktion genannt werden. Zerfällt eine Eisensteinsche Funktion überhaupt in p-adische Faktoren, so müssen diese wieder Eisensteinsche Funktionen sein. Besteht nämlich eine Gleichung:

$$F(x) = G(x)H(x) \quad (p),$$

in welcher $G(x)$ und $H(x)$ wieder als ganzzahlige Funktionen vorausgesetzt werden können, und betrachtet man sie als Kongruenz für die Primzahl p als Modul, so erhält man

$$a_0 x^\lambda \equiv (b_0 x^\mu + \cdots + b_\varrho x^{\mu-\varrho})(c_0 x^\nu + \cdots + c_\sigma x^{\nu-\sigma}) \pmod p,$$

wenn b_ϱ und c_σ die letzten durch p nicht teilbaren Koeffizienten von $G(x)$ und $H(x)$ sind. Offenbar ist diese Kongruenz nur dann möglich, wenn b_ϱ mit b_0, c_σ mit c_0 zusammenfällt, wenn also in $G(x)$ und $H(x)$ wirklich alle Koeffizienten außer b_0 und c_0 durch p teilbar sind. Derselbe Satz gilt auch natürlich bei der Zerlegung von $F(x)$ in mehr als zwei Faktoren.

Ist die Eisensteinsche Funktion $F(x)$ in h Faktoren zerlegbar, und ist

$$F(x) = G_1(x)\,G_2(x)\ldots G_h(x) \quad (p)$$

diese Zerlegung, so sind alle konstanten Glieder rechts mindestens durch p, also ihr Produkt mindestens durch p^h teilbar, und da dieses

Produkt dem konstanten Gliede von $F(x)$ gleich ist, so folgt der weitere Satz:

Eine Eisensteinsche Funktion, deren konstantes Glied genau durch p^h teilbar ist, kann höchstens in h Faktoren niedrigeren Grades zerfallen.

Ein spezieller Fall dieses Satzes ist das berühmte Theorem von Eisenstein, welches also auch in dem Bereiche der p-adischen Zahlen gilt:

Eine primitive Funktion von der Form:

$$F(x) = A_0 x^\lambda + pA_1 x^{\lambda-1} + \cdots + pA_\lambda,$$

deren konstantes Glied durch keine höhere als die erste Potenz von p teilbar ist, ist irreduktibel.

§ 5. Untersuchung der ganzzahligen Funktionen modulo p.

Die einfachen und schönen Gesetze, welche für die Teilbarkeit und Zerlegbarkeit der ganzen Funktionen mit ganzzahligen p-adischen Koeffizienten gelten, bleiben unverändert bestehen, wenn man nur ihre nullten Näherungswerte für die erste Potenz von p als Modul untersucht, und sie werden wörtlich ebenso bewiesen. Es wird daher genügen, wenn ich die hier sich ergebenden Sätze, welche später benutzt werden sollen, kurz zusammenstelle.

Da eine beliebige ganzzahlige p-adische Funktion, modulo p betrachtet, ihrem nullten Näherungswerte kongruent ist, so brauchen wir bei dieser Untersuchung nur die ganzzahligen Funktionen

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

zu betrachten, deren Koeffizienten Zahlen der Reihe $0, 1, \ldots p-1$ sind. Verbindet man zwei oder mehrere von diesen Funktionen durch die elementaren Rechenoperationen, so kann man die dann sich ergebenden ganzen oder gebrochenen Zahlkoeffizienten wieder modulo p auf ihren kleinsten Rest reduzieren, welcher wieder stets eine dieser p Zahlen ist.

Dividiert man eine Funktion $f(x)$ durch eine andere $g(x)$ und reduziert alle Zahlkoeffizienten in dieser Weise modulo p auf ihre kleinsten Reste, so erhält man eine Kongruenz

$$(1) \qquad f(x) \equiv g(x)\, g_1(x) + h(x) \pmod{p},$$

in welcher $h(x)$ von niedrigerem Grade ist, als $g(x)$; $f(x)$ heißt modulo p durch $g(x)$ teilbar, wenn $h(x) = 0$ ist.

Zwei Funktionen $f(x)$ und $g(x)$ besitzen einen größten gemeinsamen Teiler $d(x)$, welcher offenbar wieder durch das a. S. 53 angegebene Euklidische Verfahren mit der hier angegebenen Modifikation gefunden wird. Ist dieser Teiler $d(x)$ eine durch p nicht teilbare Zahl, so heißen $f(x)$ und

$g(x)$ teilerfremd modulo p. In diesem und nur in diesem Falle kann man zwei Multiplikatoren $f_1(x)$ und $g_1(x)$ so bestimmen, daß:

(2) $$f(x)g_1(x) + g(x)f_1(x) \equiv 1 \pmod p$$

ist. Aus dem a. S. 55 geführten Beweise ergibt sich nun ohne weiteres der wichtige Satz:

Zwei Funktionen $f(x)$ und $g(x)$ sind dann und nur dann teilerfremd modulo p, wenn ihre Resultante $R(f(x), g(x))$ durch p nicht teilbar ist.

Nur dann nämlich, wenn die die Resultante darstellende Determinante durch p nicht teilbar ist, kann man zwei Multiplikatoren $f_1(x)$ und $g_1(x)$ bestimmen, deren Grade niedriger sind als $f(x)$ und $g(x)$, und welche der Kongruenz

(3) $$f(x)g_1(x) + g(x)f_1(x) \equiv 1 \pmod p$$

genügen; denn durch Koeffizientenvergleichung erhält man aus (3) ein System linearer Kongruenzen modulo p, deren linke Seiten mit denjenigen der Gleichungen (4) a. S. 55 übereinstimmen, und deren Determinante eben gleich $R(f, g)$ ist.

Eine Funktion $P(x)$ heißt modulo p irreduktibel oder eine Primfunktion modulo p, wenn sie modulo p nicht einem Produkte zweier Funktionen niedrigeren Grades kongruent ist. Da für die Funktionen modulo p auch das Euklidische Verfahren zur Bestimmung des größten gemeinsamen Teilers anwendbar ist, so gelten für die Primfunktionen modulo p die a. S. 65 angegebenen drei Fundamentaltheoreme, und daraus folgt ohne weiteres der Hauptsatz:

Jede Funktion $f(x)$ läßt sich modulo p betrachtet auf eine und, abgesehen von Zahlenfaktoren auch nur auf eine Weise als Produkt von Primfunktionen darstellen.

Sind $P_1(x)$ und $P_2(x)$ zwei Primfunktionen modulo p, so ist ihre Resultante $R(P_1(x), P_2(x))$ dann und nur dann durch p teilbar, wenn beide abgesehen von einem Zahlenfaktor modulo p kongruent sind. Ist nämlich $R(P_1, P_2) \equiv 0 \pmod p$, so müssen ja $P_1(x)$ und $P_2(x)$ modulo p einen gemeinsamen Teiler haben, und da beide Primfunktionen modulo p sind, so müssen sie für diesen Modul kongruent sein.

Eine ganze Funktion $f(x) = a_0 + a_1 x + \ldots + a_\nu x^\nu$ besitzt eine Ableitung

$$f'(x) = a_1 + 2a_2 x + \cdots + \nu a_\nu x^{\nu-1},$$

deren Koeffizienten im allgemeinen nicht alle durch p teilbar sind. Sollen nämlich alle Produkte $i a_i$ die Primzahl p enthalten, so müssen alle Koeffizienten a_i, deren Index i kein Multiplum von p ist,

durch p teilbar sein, d. h. es muß $f(x)$ modulo p einer ganzen Funktion von x^p kongruent sein. Ist umgekehrt

$$(4) \qquad f(x) \equiv \alpha_0 + \alpha_1 x^p + \alpha_2 x^{2p} + \cdots + \alpha_\varrho x^{\varrho p} \pmod{p},$$

so ist $f'(x) \equiv 0 \pmod{p}$. Nun besteht aber für ein variables x die Kongruenz:

$$(\alpha_0 + \alpha_1 x + \cdots + \alpha_\varrho x^\varrho)^p \equiv \alpha_0^p + \alpha_1^p x^p + \cdots + \alpha_\varrho^p x^{p\varrho} \pmod{p},$$

denn alle übrigen Glieder können ja modulo p fortgelassen werden, weil in den zugehörigen Polynomialkoeffizienten

$$\frac{p!}{a!\, b! \cdots c!} \qquad (a + b + \cdots + c = p)$$

der Zähler durch p teilbar ist, der Nenner aber nicht. Da ferner für jede ganze Zahl α nach dem Fermatschen Satze $\alpha^p \equiv \alpha \pmod{p}$ ist, so kann die obige Kongruenz auch in der Form geschrieben werden:

$$(4\text{a}) \quad (\alpha_0 + \alpha_1 x + \cdots + \alpha_\varrho x^\varrho)^p \equiv \alpha_0 + \alpha_1 x^p + \cdots + \alpha_\varrho x^{\varrho p} \pmod{p}.$$

Wendet man diese wichtige Kongruenz auf die rechte Seite von (4) an, so ergibt sich die Richtigkeit des folgenden Theoremes:

Die Ableitung einer ganzen ganzzahligen Funktion $f(x)$ ist dann und nur dann durch die Primzahl p teilbar, wenn:

$$(4\text{b}) \qquad f(x) \equiv f_0(x)^p \pmod{p}$$

ist, wo $f_0(x)$ eine andere ganzzahlige Funktion bedeutet. Also ist die Ableitung einer Primfunktion niemals durch p teilbar.

Daraus folgt sofort, daß die Diskriminante

$$D(P(x)) = R(P(x),\ P'(x))$$

einer Primfunktion $P(x)$ niemals durch p teilbar sein kann. Ist nämlich $P(x)$ eine Primfunktion, so ist $P'(x)$ eine ganze ganzzahlige Funktion von niedrigerem Grade, deren Koeffizienten nach dem soeben bewiesenen Satze nicht sämtlich durch p teilbar sind. Wäre nun $R(P, P')$ durch p teilbar, so müßten $P(x)$ und $P'(x)$ einen gemeinsamen Teiler modulo p haben, und dies steht mit der Voraussetzung im Widerspruch, daß $P(x)$ eine Primfunktion ist.

Eine beliebige ganzzahlige Funktion $F(x)$ kann, modulo p betrachtet, lauter verschiedene Primfaktoren enthalten, oder sie kann gewisse unter ihnen mehrfach besitzen. Das letztere ist dann und nur dann der Fall, wenn sie mit ihrer Ableitung $F'(x)$, modulo p betrachtet, einen gemeinsamen Teiler hat, oder, was dasselbe ist, wenn ihre Diskriminante

$$D(F(x)) = R(F(x), F'(x))$$

durch p teilbar ist. Ist nämlich:

$$F(x) \equiv P_1(x)\, P_2(x) \cdots P_\nu(x) \pmod{p}$$

die Zerlegung der Funktion $F(x)$ in ihre gleichen oder verschiedenen Primfaktoren modulo p, so ergibt sich durch Übergang zu den Diskriminanten nach dem Satze (7) a. S. 60:

$$D(F) \equiv \pm \prod_{i=1}^{\nu} D(P_i(x)) \cdot \prod_{i>k} R^2(P_i(x), P_k(x)) \pmod{p}.$$

Da nun nach dem soeben bewiesenen Satze alle Diskriminanten $D(P_i(x))$ p nicht enthalten, und da ferner eine Resultante $R(P_i, P_k)$ dann und nur dann durch p teilbar ist, wenn $P_i(x)$ kongruent $P_k(x)$ ist, so folgt, daß $D(F(x))$ wirklich dann und nur dann durch p teilbar ist, wenn $F(x)$ mindestens einen Primteiler mehrfach enthält.

Die soeben bewiesenen Sätze benutze ich, um eine wichtige Eigenschaft der für den Bereich von p irreduktiblen Funktionen herzuleiten. Es sei nämlich $F(x)$ eine ganze Funktion mit ganzzahligen p-adischen Koeffizienten und $F_0(x)$ ihr nullter Näherungswert, so daß also:

(5) $$F(x) \equiv F_0(x) \pmod{p}$$

ist. Hat dann $F_0(x)$ modulo p betrachtet nicht lauter gleiche Primfaktoren, so zerfällt $F(x)$ sicher in zwei p-adische Faktoren niedrigeren Grades, ist also reduktibel. Unter der soeben gemachten Voraussetzung kann man nämlich $F_0(x)$ modulo p als ein Produkt $f_0(x) g_0(x)$ zweier Funktionen darstellen, welche keinen einzigen Primfaktor modulo p gemeinsam haben, denn man braucht ja nur jeden mehrfachen Faktor $P^{\alpha}(x)$ von $F_0(x)$ entweder ganz zu $f_0(x)$ oder ganz zu $g_0(x)$ zu fügen. Dann folgt also aus (5) die Kongruenz:

(5a) $$F(x) \equiv f_0(x) g_0(x) \pmod{p},$$

und es ist $R(f_0(x), g_0(x))$ durch p nicht teilbar, weil jene Funktionen teilerfremd sind. Nach dem a. S. 71 (1) bewiesenen Satze entspricht also dieser Kongruenz (4a) eine Zerlegung:

(5b) $$F(x) = f(x) g(x) \quad (p)$$

von $F(x)$ in zwei p-adische Faktoren $f(x)$ und $g(x)$, deren Näherungswerte eben jene Funktionen $f_0(x)$ und $g_0(x)$ sind. Hieraus ergibt sich also der wichtige Satz:

> Eine ganzzahlige Funktion mit p-adischen Koeffizienten ist sicher reduktibel, wenn ihr nullter Näherungswert noch modulo p verschiedene Primfaktoren hat.
>
> Der nullte Näherungswert einer irreduktiblen p-adischen Funktion ist also modulo p betrachtet entweder selbst irreduktibel oder die Potenz einer modulo p irreduktiblen Funktion.

So ist z. B. eine irreduktible Eisensteinsche Funktion

$$f(x) = A_0 x^\lambda + pA_1 x^{\lambda-1} + \cdots + pA_\lambda$$

modulo p betrachtet kongruent $A_0 x^\lambda$, d. h. sie ist der λ^{ten} Potenz des Linearfaktors x kongruent.

§ 6. Anwendungen. Die $(p-1)^{\text{ten}}$ Wurzeln der Einheit im Gebiete der p-adischen Zahlen.

Als Anwendung der in diesem Kapitel bewiesenen Sätze untersuche ich jetzt einige spezielle Gleichungen, welche z. T. später benutzt werden sollen. Ich betrachte zuerst die reine Gleichung:

(1) $$x^{p-1} - 1 = 0 \quad (p)$$

und zeige, daß ihre linke Seite im Gebiete der p-adischen Zahlen gleich dem Produkt von $p-1$ Linearfaktoren ist. Ihr nullter Näherungswert zerfällt nämlich, modulo p betrachtet, nach dem Fermatschen Satze in $p-1$ Linearfaktoren; bekanntlich besteht nämlich für ein variables x die Kongruenz:

(1a) $$x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-\overline{p-1}) \pmod{p},$$

und da alle diese Linearfaktoren modulo p teilerfremd sind, weil allgemein:

$$R(x-i,\ x-k) = i-k$$

durch p nicht teilbar ist, so folgt nach dem a. S. 79 unten bewiesenen Satze, daß $x^{p-1}-1$ für den Bereich von p ebenfalls in $p-1$ p-adische Linearfaktoren $(x-\omega_k)$ zerfällt, deren nullte Näherungswerte bzw. $(x-1), (x-2), \ldots (x-\overline{p-1})$ sind. Also besteht für ein variables x eine Gleichung:

(2) $$x^{p-1} - 1 = (x-\omega_1)(x-\omega_2)\ldots(x-\omega_{p-1}) \quad (p),$$

wo allgemein:

(2a) $$\omega_k = k + pa_k$$

ist, und a_k eine ganze p-adische Zahl bedeutet. Speziell ist

$$\omega_1 = 1,$$

d. h. es ist $a_1 = 0$, da $1^{p-1} = 1$ ist. Dagegen sind die anderen Zahlen $a_2, a_3 \ldots$ von Null verschieden, da zwar $k^{p-1} \equiv 1 \pmod{p}$ aber nicht gleich Eins ist.

Die Gleichung

$$x^{p-1} - 1 = 0$$

besitzt also genau $p-1$ p-adische Wurzeln, deren Anfangsziffern bzw. gleich $1, 2, \ldots p-1$ sind, und welche leicht mit jeder vorgegebenen Genauigkeit berechnet werden können. Diese Zahlen heißen die $(p-1)^{\text{ten}}$ *p-adischen Wurzeln der Einheit.*

So besitzt z. B. die Gleichung:

$$x^6 - 1 = 0 \quad (7)$$

sechs heptadische Wurzeln, welche bis zur zweiten Stelle genau die folgenden Werte haben:

$$\begin{array}{ll} \omega_1 = 1{,}00\ldots & \omega_4 = 4{,}20\ldots \\ \omega_2 = 2{,}46\ldots & \omega_5 = 5{,}20\ldots \quad (7) \\ \omega_3 = 3{,}46\ldots & \omega_6 = 6{,}66\ldots, \end{array}$$

und die Gleichung:

$$x^{12} - 1 = 0 \quad (13)$$

hat die folgenden zwölf Wurzeln:

$$\begin{array}{llll} \omega_1 = 1,\ 0\ 0\ldots, & \omega_4 = 4, 11\ 6\ldots, & \omega_7 = 7, 11\ \ 3\ldots, & \omega_{10} = 10,\ 1\ \ 6\ldots \\ \omega_2 = 2,\ 6\ 2\ldots, & \omega_5 = 5,\ 5\ 1\ldots, & \omega_8 = 8,\ \ 7\ 11\ldots, & \omega_{11} = 11,\ 6\ 10\ldots \quad (13) \\ \omega_3 = 3, 11\ 6\ldots, & \omega_6 = 6,\ 1\ 9\ldots, & \omega_9 = 9,\ \ 1\ \ 6\ldots, & \omega_{12} = 12, 12\ 12\ldots, \end{array}$$

wobei zu bemerken ist, daß bei der Grundzahl 13 die Zahlen 10, 11, 12 wieder einfache Ziffern bedeuten. Ist p eine ungerade Zahl, so ist außer $\omega_1 = 1{,}00\ldots$ nur noch

$$\omega_{p-1} = p-1,\ p-1\ p-1\ldots = -1$$

periodisch, während die anderen Wurzeln offenbar nicht periodisch sind.

Es sei nun ω irgend eine von den $p-1$ Wurzeln unserer Gleichung; dann sind alle p-adischen Zahlen:

(3) $$1, \omega, \omega^2, \ldots$$

ebenfalls Wurzeln derselben Gleichung, weil allgemein:

$$(\omega^k)^{p-1} = (\omega^{p-1})^k = 1 \quad (p)$$

ist. Da diese Gleichung nur $p-1$ verschiedene Wurzeln hat, so können nicht alle Potenzen von ω voneinander verschieden sein. Sind ω^r und ω^{r+d} die beiden ersten Wurzeln in dieser Reihe, welche einander gleich sind, so folgt aus der Gleichung:

$$\omega^{r+d} = \omega^r \quad (p)$$

sofort, daß $\omega^d = 1$ sein muß. Es ist also 1 die erste wiederkehrende Wurzel in der Reihe (3), und sie besteht offenbar aus dem sich stets wiederholenden Zyklus:

(3a) $$1, \omega, \omega^2, \ldots \omega^{d-1}, 1, \omega, \omega^2, \ldots \omega^{d-1}, \ldots,$$

in welchem nur die ersten d Wurzeln voneinander verschieden sind. Wir sagen, die Wurzel ω gehört zum Exponenten d, wenn ω^d die kleinste Potenz von ω ist, welche gleich Eins wird. Gehört ω zum Exponenten d, so sind die Potenzen $1, \omega^d, \omega^{2d}, \ldots$ die einzigen, welche gleich Eins sind, d. h. eine Potenz von ω ist dann und nur dann gleich

Eins, wenn ihr Exponent durch d teilbar ist. Da aber alle Zahlen ω der Gleichung $\omega^{p-1} = 1$ genügen, so folgt endlich, daß jeder der Exponenten d ein Teiler von $p-1$ sein muß.

Jede der $p-1$ $(p-1)^{\text{ten}}$ p-adischen Wurzeln der Einheit gehört also zu einem Exponenten, welcher ein Teiler von $p-1$ ist.

Gehört

$$\omega_k = k + p a_k$$

zum Exponenten d, so ist:

$$\omega_k^d \equiv k^d \equiv 1, \quad (\text{mod } p)$$

während alle niedrigeren Potenzen von ω_k, also auch von k, nicht kongruent Eins sind, da ja $\omega, \omega^2, \dots \omega^{d-1}$ andere Anfangsglieder als 1 haben. Wir können also sagen:

Eine Wurzel ω_k gehört dann und nur dann zu einem Exponenten d, wenn ihr Anfangsglied k modulo p im Sinne der elementaren Arithmetik zu demselben Exponenten gehört.

Nun gibt es bekanntlich stets $\varphi(d)$ modulo p inkongruente Zahlen k, welche zu einem gegebenen Teiler d von $p-1$ als Exponenten gehören.

Also gibt es auch stets genau $\varphi(d)$ verschiedene $(p-1)^{\text{te}}$ Wurzeln der Einheit, welche zu einem gegebenen Teiler d von $p-1$ als Exponenten gehören.

Speziell gibt es also genau $\varphi(p-1)$ s. g. primitive $(p-1)^{\text{te}}$ Wurzeln der Einheit, d. h. solche Wurzeln ω, welche zu dem Exponenten $p-1$ selbst gehören. Eine Wurzel

$$\omega = g + p a_g$$

ist dann und nur dann eine primitive Einheitswurzel, wenn ihr Anfangsglied g eine primitive Kongruenzwurzel modulo p ist.

Ist ω eine primitive Einheitswurzel, so sind die $p-1$ Potenzen:

$$1, \omega, \omega^2, \dots \omega^{p-2}$$

lauter voneinander verschiedene Wurzeln unserer Gleichung, und da sie nicht mehr als $p-1$ Wurzeln besitzt, so folgt der Satz:

Ist ω eine der $\varphi(p-1)$ primitiven $(p-1)^{\text{ten}}$ Einheitswurzeln, so sind alle übrigen in der Reihe $1, \omega, \omega^2, \dots \omega^{p-2}$ enthalten.

Natürlich hätte die Existenz der primitiven Kongruenzwurzeln g modulo p hier auch direkt hergeleitet werden können, ohne die entsprechenden Resultate der elementaren Arithmetik vorauszusetzen; dies werde jedoch dem Leser überlassen.

So ist für die sechsten Wurzeln der Einheit für den Bereich von 7:

$$\omega = 3, 46 \dots \quad (7)$$

eine primitive Wurzel, und man überzeugt sich durch einfaches Multiplizieren leicht, daß

$$\begin{array}{ll} 1 = 1,00\ldots, & \omega^3 = 6,66\ldots, \\ \omega = 3,46\ldots, & \omega^4 = 4,20\ldots, \\ \omega^2 = 2,46\ldots, & \omega^5 = 5,20\ldots. \end{array} \qquad (7)$$

ist. Ebenso ist für die zwölften Einheitswurzeln für den Bereich von 13:

$$\omega = 2,62\ldots \qquad (13)$$

eine primitive Wurzel, und man erhält hier alle Wurzeln in der folgenden Reihenfolge:

$$\begin{array}{lll} 1 = 1,\ 0\ \ 0\ldots, & \omega^4 = 3,11\ \ 6\ldots, & \omega^8 = 9,\ 1\ 6\ldots, \\ \omega = 2,\ 6\ \ 2\ldots, & \omega^5 = 6,\ 1\ \ 9\ldots, & \omega^9 = 5,\ 5\ 1\ldots, \\ \omega^2 = 4,11\ \ 6\ldots, & \omega^6 = 12,12\ 12\ldots, & \omega^{10} = 10,\ 1\ 6\ldots, \\ \omega^3 = 8,\ 7\,11\ldots, & \omega^7 = 11,\ 6\ 10\ldots, & \omega^{11} = 7,11\ 3\ldots. \end{array} \qquad (13)$$

Die $p-1$ Wurzeln $\overline{\omega}_0, \overline{\omega}_1, \ldots \overline{\omega}_{p-2}$ der Kreisteilungsgleichung (1) lassen sich bekanntlich ihrer Größe nach folgendermaßen darstellen:

$$\overline{\omega}_0 = 1, \quad \overline{\omega}_1 = \cos\frac{2\pi}{p-1} + i\sin\frac{2\pi}{p-1}, \cdots \quad \overline{\omega}_k = \cos\frac{2k\pi}{p-1} + i\sin\frac{2k\pi}{p-1}, \cdots,$$

und schon hieraus folgt mit Hilfe des Moivreschen Satzes, daß:

$$\overline{\omega}_k = \overline{\omega}_1^{\,k} \qquad (k = 0, 1, \cdots p-2)$$

ist. Dasselbe kann aber genau wie vorher für die p-adischen Wurzeln so erschlossen werden: Ist $\overline{\omega}$ irgend eine der $p-1$ Wurzeln, so sind alle komplexen Zahlen $(1, \overline{\omega}, \overline{\omega}^2, \ldots)$ ebenfalls Wurzeln, und hieraus folgt genau wie vorher der Satz:

Jede $(p-1)^{\text{te}}$ Wurzel der Einheit gehört zu einem Exponenten, welcher ein Teiler von $(p-1)$ ist. Ist umgekehrt d irgend ein Teiler von $p-1$, so gibt es genau $\varphi(d)$ $(p-1)^{\text{te}}$ Wurzeln der Einheit, welche zum Exponenten d gehören. Speziell gibt es also genau $\sigma = \varphi(p-1)$ s. g. primitive $(p-1)^{\text{te}}$ Wurzeln der Einheit, welche zum Exponenten $p-1$ gehören. Ist $\overline{\omega}$ eine solche, so sind alle $p-1$ Einheitswurzeln in der Reihe: $(1, \overline{\omega}, \overline{\omega}^2, \ldots \overline{\omega}^{p-2})$ enthalten.

Eine dieser primitiven $(p-1)^{\text{ten}}$ Einheitswurzeln ist eben

$$\overline{\omega}_1 = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p};$$

Sind $\overline{\omega}^{(1)}, \overline{\omega}^{(2)}, \ldots \overline{\omega}^{(\sigma)}$ alle $\sigma = \varphi(p-1)$ primitiven $(p-1)^{\text{ten}}$ Einheits-

wurzeln, so genügen diese, wie in der Algebra sehr einfach gezeigt wird*), einer Gleichung:

(4) $$g(x) = (x - \overline{\omega}^{(1)})(x - \overline{\omega}^{(2)}) \cdots (x - \overline{\omega}^{(\sigma)}) = 0$$

mit gewöhnlichen ganzzahligen Koeffizienten, deren linke Seite natürlich ein Teiler von $x^{p-1} - 1$ und außerdem im Gebiete der rationalen Zahlen irreduktibel ist. Dieselbe Gleichung, für den Bereich von p betrachtet, enthält alle und nur die $\varphi(p-1)$ primitiven p-adischen Wurzeln, $\omega^{(1)}, \omega^{(2)} \ldots \omega^{(\sigma)}$, d. h. es ist für den Bereich von p:

(4a) $$g(x) = (x - \omega^{(1)})(x - \omega^{(2)}) \cdots (x - \omega^{(\sigma)}) \qquad (p).$$

Der einfache Beweis dieses Satzes werde dem Leser überlassen.

Eine Verallgemeinerung der hier betrachteten Funktionen $x^{p-1} - 1$ oder, was im wesentlichen dasselbe ist, der Funktionen

(5) $$H_1(x) = x^p - x = x(x-1)(x-\omega) \cdots (x - \omega^{p-2}) \qquad (p)$$

sind die Funktionen:

(5a) $$H_f(x) = x^{p^f} - x,$$

welche uns später in der Theorie der algebraischen Zahlen begegnen werden. Da ihre Ableitung:

$$H_f'(x) = p^f x^{p^f - 1} - 1 \equiv -1 \pmod{p}$$

ist, so kann $H_f(x)$ keinen Primteiler modulo p mehrfach enthalten, weil ja dieser sonst auch in -1 enthalten sein müßte. Also ist die Diskriminante von $H_f(x)$ durch p nicht teilbar (s. S. 78 letzter Absatz).

Hieraus folgt, daß die Primfaktoren modulo p von H_f alle voneinander verschieden sind, und daraus ergibt sich weiter, daß bei der Zerlegung:

$$H_f(x) = g_1(x)\, g_2(x) \cdots g_\nu(x) \qquad (p)$$

von $H_f(x)$ in irreduktible p-adische Faktoren alle Funktionen $g_i(x)$ auch modulo p betrachtet irreduktibel und teilerfremd sind.

Während die vorher betrachteten einfachsten Funktionen

$$H_1(x) = x^p - x$$

in p p-adische Linearfaktoren zerfallen, enthalten die Funktionen $H_f(x)$, wie wir sehen werden, lauter irreduktible p-adische Faktoren, deren Grad gleich f oder gleich einem Teiler von f ist. Schon hier zeigt sich also, daß die Wurzeln der Gleichung

$$H_f(x) = x^{p^f} - x = x(x^{p^f - 1} - 1) = 0 \qquad (p),$$

d. h. die $(p^f - 1)^{\text{ten}}$ Wurzeln der Einheit, nicht sämtlich als p-adische Zahlen darstellbar sind. Wir werden später sehen, wie das Gebiet

*) Vgl. z. B. H. Weber, Algebra Bd. I, §§ 141 und 174.

der p-adischen Zahlen erweitert werden muß, damit auch sie darin enthalten sind.

§ 7. Die Auflösung der reinen Gleichungen im Gebiete der p-adischen Zahlen. Theorie der Potenzreste.

Ich wende mich zunächst noch zu den $(p-1)^{\text{ten}}$ Einheitswurzeln, um mit ihrer Hilfe die p-adischen Zahlen in einer für ihre multiplikative Zusammensetzung besonders geeigneten Weise darzustellen. Zu diesem Zwecke führe ich den neuen Begriff der **Haupteinheit** ein und bezeichne so jede Einheit:

$$e = 1, a_1 a_2 \cdots,$$

deren Anfangsglied gleich Eins ist. Das Produkt und der Quotient zweier Haupteinheiten ist offenbar wieder eine Haupteinheit. Jede andere Einheit

$$B_0 = b_0, b_1 b_2 \cdots$$

unterscheidet sich von dieser Haupteinheit nur um eine $(p-1)^{\text{te}}$ Einheitswurzel als Faktor. Ist nämlich ω eine primitive $(p-1)^{\text{te}}$ Wurzel der Einheit, und

$$\omega^\beta = b_0 + p\bar{b}$$

die Einheitswurzel, welche dieselbe Anfangsziffer hat wie B_0, so ist der Quotient

$$\frac{B_0}{\omega^\beta} = \frac{b_0, b_1 b_2 \cdots}{b_0 + p\bar{b}} = 1, a_1 a_2 \ldots \quad (p)$$

eine Haupteinheit, weil der nullte Näherungswert dieses Quotienten modulo p kongruent $\frac{b_0}{b_0} = 1$ ist. Es ergibt sich also der Satz:

Jede p-adische Einheit B ist in der Form:

(1) $$B_0 = \omega^\beta e$$

darstellbar, wo e eine Haupteinheit und ω eine primitive $(p-1)^{\text{te}}$ Wurzel der Einheit bedeutet. Allgemeiner kann also jede p-adische Zahl $B = p^\varrho B_0$ in der Form:

(1a) $$B = p^\varrho \omega^\beta e$$

dargestellt werden.

Zwei in dieser Form geschriebene Zahlen

$$B = p^\varrho \omega^\beta e, \qquad B' = p^{\varrho'} \omega^{\beta'} e'$$

sind dann und nur dann einander gleich, wenn

(1b) $$\varrho = \varrho', \quad \beta \equiv \beta' \ (\text{mod}\, p-1) \quad \text{und} \quad e = e' \quad (p)$$

ist.

Ehe ich mit Hilfe dieser Betrachtungen die allgemeine binomische Gleichung im Gebiete der p-adischen Zahlen auflöse, beweise ich noch den folgenden Hilfssatz:

Ist $e = 1, e_1 e_2 \cdots$ irgend eine Haupteinheit und μ eine durch p nicht teilbare Zahl, so gibt es eine einzige Haupteinheit $\varepsilon = 1, \varepsilon_1 \varepsilon_2 \cdots$, welche gleich $\sqrt[\mu]{e}$ ist, welche also der Gleichung:

$$\varepsilon^\mu = e \qquad (p)$$

genügt.

Setzt man nämlich in der Gleichung:

$$f(x) = x^\mu - e = 0$$

$x = 1$, so wird $f(1) = 1 - e = -0, e_1 e_2 \cdots$ durch p teilbar. Da aber $f'(1) = \mu$ n. d. V. durch p nicht teilbar, also $\frac{f(1)}{(f'(1))^2}$ von positiver Ordnung ist, so besitzt nach dem a. S. 71 (3) bewiesenen Satze, die obige Gleichung eine einzige Wurzel, deren nullter Näherungswert gleich 1 ist, d. h. es gibt eine einzige Haupteinheit $\varepsilon = 1, \varepsilon_1 \varepsilon_2 \cdots$, deren μ^{te} Potenz gleich e ist.

Dieses Resultat benutze ich zur Auflösung der allgemeinen reinen Gleichung:

(2) $$x^\mu = B \qquad (p)$$

im Gebiet der p-adischen Zahlen für den Fall, daß der Exponent μ nicht durch p teilbar ist. Es sei:

(2a) $$B = p^\varrho \omega^\beta e,$$

und die unbekannte Zahl x werde gleich

(2b) $$x = p^\sigma \omega^\xi \varepsilon$$

gesetzt. Dann ergibt die Substitution dieser Werte in (2) für die Unbekannten σ, ξ und ε die Gleichung:

$$p^{\sigma\mu} \omega^{\xi\mu} \varepsilon^\mu = p^\varrho \omega^\beta e \qquad (p),$$

und diese ist nach (1b) dann und nur dann erfüllt, wenn:

$$\sigma\mu = \varrho, \qquad \mu\xi \equiv \beta \mod (p-1), \qquad \varepsilon^\mu = e \qquad (p)$$

ist. Nach dem soeben geführten Beweise ist die dritte Gleichung stets lösbar und bestimmt die Haupteinheit ε eindeutig, die erste ergibt dann und nur dann ein ganzzahliges σ, wenn ϱ durch μ teilbar ist. Zur vollständigen Lösung der mittleren Kongruenz bezeichnen wir mit $d = (\mu, p-1)$ den größten gemeinsamen Teiler von μ und $p - 1$. Dann besitzt diese Kongruenz bekanntlich dann und nur dann eine

Lösung, wenn β auch durch d teilbar ist. Ist dies der Fall, und setzen wir

$$\mu = d\mu_0, \quad \beta = d\beta_0, \quad p-1 = dd_0,$$

so ergibt sich nach Wegheben dieses gemeinsamen Faktors die einfache Kongruenz für ξ:

$$\mu_0 \xi \equiv \beta_0 \pmod{d_0},$$

wo jetzt μ_0 und d_0 teilerfremd sind. Eine solche Kongruenz hat bekanntlich eine modulo d_0 eindeutig bestimmte Lösung:

$$\xi_0 \equiv \frac{\beta_0}{\mu_0} \pmod{d_0},$$

und aus ihr ergeben sich für die ursprüngliche Kongruenz modulo $p-1 = dd_0$ genau d inkongruente Lösungen, nämlich:

$$\xi_0, \quad \xi_0 + d_0, \quad \xi_0 + 2d_0, \cdots \xi_0 + (d-1)d_0.$$

Wir wollen eine Zahl B einen μ^{ten} Potenzrest für den Bereich von p nennen, wenn sie die μ^{te} Potenz einer p-adischen Zahl ist, wenn also die Gleichung $x^\mu = B$ eine p-adische Lösung hat. Dann können wir das soeben gefundene Resultat in dem folgenden einfachen Satze aussprechen:

Ist μ durch p nicht teilbar, so ist die Zahl $B = p^\varrho \omega^\beta e$ dann und nur dann μ^{ter} Potenzrest für den Bereich von p, wenn ihre Ordnungszahl ϱ durch μ, und wenn zugleich der Exponent β durch $d = (\mu, p-1)$ teilbar ist, und zwar besitzt dann $\sqrt[\mu]{B}$ genau d voneinander verschiedene p-adische Werte, welche sich voneinander nur um Potenzen von $\omega^{\frac{p-1}{d}}$ unterscheiden.

Für $\mu = 2$ und $\mu = 3$ erhält dieser allgemeine Satz die folgende einfachere Form:

Eine Zahl $B = p^\varrho \omega^\beta e$ ist dann und nur dann quadratischer Rest für den Bereich einer ungeraden Primzahl p, wenn die beiden Exponenten ϱ und β gerade sind.

Eine Zahl $B = p^\varrho \omega^\beta e$ ist kubischer Rest, wenn ϱ durch 3 und β durch $d = (3, p-1)$ teilbar ist, und die Gleichung

$$x^3 - B = 0 \quad (p)$$

besitzt in diesem Falle genau d verschiedene p-adische Wurzeln. Ist also p von der Form $3n+1$, so ist $d = 3$, d. h. B ist kubischer Rest, wenn ϱ und β durch drei teilbar sind, und $\sqrt[3]{B}$ hat drei p-adische Zahlwerte. Ist dagegen $p = 3n+2$, also $d = 1$, so ist B kubischer Rest zu p, wenn ϱ ein Multiplum von 3 ist, während β beliebig sein kann. In diesem

Falle zerfällt $x^3 - B$ nicht in drei p-adische Linearfaktoren, sondern nur in je einen Faktor ersten und zweiten Grades.

Zum Abschluß dieser Übungsbeispiele untersuche ich noch die Frage, unter welcher Bedingung eine Zahl $B = p^\varrho \omega^\beta e$ p^{ter} Potenzrest ist, d. h. wann die Gleichung:

(3) $$x^p - B = 0 \quad (p)$$

eine Wurzel besitzt. Setzt man wieder $x = p^\sigma \omega^\xi \varepsilon$, so muß auch hier

(3a) $$\sigma p = \varrho, \quad \omega^{p\xi} = \omega^\beta, \quad \varepsilon^p = e$$

sein; da aber $\omega^p = \omega$ ist, so muß eben $\xi = \beta$ sein, wodurch ξ stets eindeutig bestimmt wird. Also treten hier nur die beiden Bedingungen auf, daß ϱ durch p teilbar ist, und daß die Haupteinheit ε so gewählt werden kann, daß sie die Gleichung:

(3b) $$f(x) = x^p - e = 0 \quad (p)$$

befriedigt, wo $e = 1, e_1 e_2 \ldots$ ist. Aber diese Gleichung ist hier nicht stets lösbar, sondern im allgemeinen nur dann, wenn $e = 1{,}0 e_2 \ldots$, wenn also $e_1 = 0$ ist. Setzt man nämlich $x = y + 1$, so genügt y der Gleichung

$$(y+1)^p - 1, e_1 e_2 \ldots = y^p + p y^{p-1} + \frac{p(p-1)}{1 \cdot 2} y^{p-2} + \cdots + p y - 0, e_1 e_2 \cdots = 0,$$

und ihre linke Seite ist eine Eisensteinsche Funktion, da alle ihre Koeffizienten mindestens durch p teilbar sind. Ist also $e_1 > 0$, so ist das konstante Glied nur durch die erste Potenz von p teilbar, also ist dann ihre linke Seite nach dem a. S. 76 oben bewiesenen Satze irreduktibel; sie besitzt mithin keinen p-adischen Linearfaktor.

Es sei also jetzt $e = 1, 0\, e_2 \ldots$, so beweise ich wieder, daß die Gleichung (3b) für jede **ungerade** Primzahl p eine einzige Haupteinheit ε als Lösung hat. In der Tat besitzt die Näherungskongruenz:

(4) $$f^{(3)}(x) = x^p - 1{,}0 e_2 \equiv 0 \pmod{p^3}$$

die Lösung $\xi_0 = 1, e_2$, denn es ist ja:

$$\begin{aligned} \xi_0^p = (1 + p e_2)^p &= 1 + p^2 e_2 + \frac{p(p-1)}{1 \cdot 2} p^2 e_2^2 + \cdots \\ &\equiv 1 + p^2 e_2 = 1{,}0\, e_2 \pmod{p^3}, \end{aligned}$$

weil alle folgenden Glieder mindestens durch p^3 teilbar sind.

Also ist $1, e_2 = \xi_0$ eine Zahl, für welche $f(\xi_0)$ durch p^3 teilbar ist. Da aber $f'(\xi_0) = p \xi_0^{p-1}$ genau durch p teilbar, also $\frac{f(\xi_0)}{f'(\xi_0)^2}$ von positiver Ordnung ist, so besitzt die obige Gleichung eine einzige Wurzel ξ, deren Näherungswert $\xi_0 = 1, e_2$, welche also eine Haupteinheit ist. Da

hiernach die obige Gleichung in diesem Falle stets eine und nur eine Lösung zuläßt, so ergibt sich der folgende sog. Ergänzungssatz in der Theorie der Potenzreste:

Eine Zahl $B = p^{\varrho}\omega^{\beta}e$ ist dann und nur dann p^{ter} Potenzrest zu der ungeraden Primzahl p, wenn die Ordnungszahl $\varrho = p\varrho_0$ ein Vielfaches von p ist und die Haupteinheit e die Form:

$$e = 1,0e_2\cdots = 1 + p^2 g$$

besitzt. In diesem Falle gibt es nur eine p-adische Zahl

$$p^{\varrho_0}\omega^{\beta'}\cdot e^{\frac{1}{p}},$$

welche für den Bereich von p gleich $\sqrt[p]{B}$ ist.

Eine kleine Modifikation tritt nur für $p = 2$ ein; denn in diesem Falle hat die Näherungskongruenz (4):

$$f^{(2)}(x) = x^2 - 1,0e_2 \equiv 0 \pmod{2^3}$$

nur dann eine Lösung, wenn auch $e_2 = 0$ ist. Setzt man nämlich $x = 1 + 2g$, so wird ja

$$x^2 - 1,0e_2 = (1+2g)^2 - 1,0e_2 = 1 + 4g + 4g^2 - 1,0e_2 = 4g(g+1) - 4e_2,$$

und die Zahl $4(g(g+1) - e_2)$ ist, wie auch g gewählt werde, nicht durch 2^3 teilbar, falls $e_2 = 1$ ist; ist aber $e_2 = 0$, so erhält man für $g = 0$ und $g = 1$ je einen Näherungswert unserer Kongruenz. Also muß hier auch $e_2 = 0$ sein, und da für $p = 2$ jede Einheit eine Haupteinheit also $\omega = 1$ ist, erhalten wir für diese Primzahl noch den Zusatz:

Eine Zahl $B = 2^{\varrho}\cdot e$ ist in bezug auf 2 quadratischer Rest, wenn ϱ gerade ist, während die Einheit e die Form:

$$e = 1,00e_3\cdots = 1 + 8a$$

hat, und in diesem Falle hat $\sqrt{B}$ zwei dyadische Werte.

Ähnliche Sätze bestehen, wenn $\mu = p^2$ oder einer höheren Potenz von p gleich ist, doch soll auf die Herleitung derselben an dieser Stelle nicht eingegangen werden.

§ 8. Die Darstellung der Gleichungswurzeln für den Bereich von p und nach ihrer Größe.

Im § 5 des zweiten Kapitels war gezeigt worden, daß und wie sich jede rationale Zahl auf eine einzige Weise in eine im gewöhnlichen Sinne konvergente Reihe

$$a_{\varrho}p^{\varrho} + a_{\varrho+1}p^{\varrho+1} + a_{\varrho+2}p^{\varrho+2} + \cdots$$

mit modulo p ganzen rationalen Koeffizienten so entwickeln läßt, daß sie dieser rationalen Zahl sowohl ihrer Größe nach, als auch für den Be-

reich von p gleich ist. Auch für die algebraischen Zahlen, d. h. für die Wurzeln einer beliebigen ganzzahligen Gleichung:

(1) $$f(x) = 0,$$

mögen diese nun reell oder komplex sein, gilt genau derselbe Satz, aber nur unter der Voraussetzung, daß die Gleichung

(1a) $$f(x) = 0 \quad (p)$$

mindestens eine p-adische Wurzel besitzt, d. h. daß ihre linke Seite für den Bereich von p mindestens einen p-adischen Linearfaktor hat.

In der Tat, sei:

(2) $$f(x) = (x - \xi) f_1(x) \quad (p),$$

wo

(2a) $$\xi = \xi_0 + \xi_1 p + \cdots$$

eine p-adische reduzierte Zahl bedeutet, welche ich der Einfachheit wegen als eine modulo p ganze Zahl annehme. Es sei ferner α eine der n Wurzeln, welche die irreduktible Gleichung $f(x) = 0$ ihrer Größe nach besitzt, und zwar möge α zunächst eine gewöhnliche reelle Zahl sein. Dann folgt aus dem a. S. 43 bewiesenen Satze, daß man diese stets in eine konvergente Reihe:

$$\alpha = \alpha_0 + \alpha_1 p + \cdots$$

entwickeln kann, deren Koeffizienten α_i rationale, aber modulo p ganze Zahlen, und die ferner so gewählt sind, daß für den Bereich von p

(3) $$\alpha = \xi \quad (p)$$

ist, daß nämlich die Kongruenzen:

(3a) $$\begin{aligned} \alpha_0 &\equiv \xi_0 \pmod{p}, \\ \alpha_0 + \alpha_1 p &\equiv \xi_0 + \xi_1 p \pmod{p^2}, \\ \alpha_0 + \alpha_1 p + \alpha_2 p^2 &\equiv \xi_0 + \xi_1 p + \xi_2 p^2 \pmod{p^3}, \\ &\cdots\cdots\cdots \end{aligned}$$

sämtlich erfüllt sind. Genau dasselbe ist möglich, wenn:

$$\alpha = \beta + \gamma i$$

eine komplexe Wurzel unserer Gleichung ist; auch dann kann man α in eine konvergente Reihe

(3b) $$\alpha = (\beta_0 + \gamma_0 i) + p(\beta_1 + \gamma_1 i) + \cdots$$

entwickeln, deren Koeffizienten modulo p ganze rationale komplexe Brüche sind, und für die der Reihe nach die Kongruenzen:

(3c) $$\begin{aligned} \beta_0 + \gamma_0 i &\equiv \xi_0 \pmod{p}, \\ (\beta_0 + \gamma_0 i) + p(\beta_1 + \gamma_1 i) &\equiv \xi_0 + \xi_1 p \pmod{p^2}, \\ &\cdots\cdots\cdots \end{aligned}$$

sämtlich erfüllt sind.

Besitzt dagegen die Gleichung (1a) für den Bereich von p keine p-adische Wurzel ξ, so ist es auch unmöglich, eine der Gleichungswurzeln α in eine konvergente p-adische Reihe $\alpha_0 + \alpha_1 p + \cdots$ so zu entwickeln, daß ihre Näherungswerte die Gleichung

(3d) $$f(x) = 0 \quad (p)$$

mit jeder vorgegebenen Annäherung befriedigen. Wäre dies nämlich für die nicht reduzierte p-adische Zahl

$$\alpha = \sum \alpha_i p^i$$

der Fall, und ist für den Bereich von p

$$\alpha = \sum \alpha_i p^i = \sum \xi_i p^i = \xi \quad (p)$$

die reduzierte Form jener Zahl, so ist auch die reduzierte Zahl ξ eine Wurzel unserer Gleichung (3d), d. h. die Funktion $f(x)$ würde entgegen unserer Voraussetzung für den Bereich von p den Linearfaktor $x - \xi$ besitzen. Es besteht also der Satz:

Ist

$$f(x) = 0$$

eine beliebige Gleichung n^{ten} Grades, so können ihre Wurzeln α sämtlich dann und nur dann in konvergente p-adische Reihen entwickelt werden, welche auch für den Bereich von p Wurzeln jener Gleichung sind, wenn jene Gleichung für den Bereich von p mindestens eine p-adische Wurzel ξ besitzt; und zwar kann dann jede der n Gleichungswurzeln $\alpha_1, \alpha_2, \ldots \alpha_n$ so entwickelt werden, daß sie für den Bereich von p gleich ξ wird.

Die Kreisteilungsgleichung des $(p-1)^{\text{ten}}$ Grades:

(4) $$x^{p-1} - 1 = 0$$

besitzt z. B. ihrer Größe nach die $p - 1$ Wurzeln:

(4a) $$1, \ \overline{\omega}, \ \overline{\omega}^2, \ldots \ \overline{\omega}^{p-2},$$

wo

(4b) $$\overline{\omega} = \cos\frac{2\pi}{p-1} + i \sin\frac{2\pi}{p-1}$$

ist. A. S. 82 unten wurde ferner bewiesen, daß dieselbe Gleichung für den Bereich der Primzahl p genau $p - 1$ p-adische Wurzeln hat, welche der Reihe nach gleich:

(4c) $$1, \ \omega, \ \omega^2, \cdots \ \omega^{p-2}$$

gesetzt werden können, wenn ω irgend eine der $\varphi(p-1)$ primitiven p-adischen Wurzeln dieser Gleichung ist.

Das soeben gefundene Resultat läßt sich nun für unseren Fall so aussprechen:

Die $p-1$ $(p-1)^{\text{ten}}$ Wurzeln der Einheit

$$\omega_0,\ \omega_1,\ \ldots\ \omega_{p-2}$$

können stets so in konvergente p-adische Reihen entwickelt werden, daß allgemein für den Bereich von p:

$$\omega_0 = \omega^{i_0},\ \omega_1 = \omega^{i_1}, \ldots \omega_{p-2} = \omega^{i_{p-2}} \qquad (p),$$

und daß ferner der Größe nach:

$$\omega_0 = \bar{\omega}^{k_0},\ \omega_1 = \bar{\omega}^{k_1}, \cdots \omega_{p-2} = \bar{\omega}^{k_{p-2}}$$

ist, wo $(i_0, i_1, \ldots i_{p-2})$ und $(k_0, k_1, \ldots k_{p-2})$ zwei beliebige Permutationen der Zahlen $0, 1, \ldots p-2$ bedeuten.

Wir würden so also $(p-1)!$ verschiedene mögliche Entwicklungen der $(p-1)$ Wurzeln ω_i in p-adische Reihen erhalten. Unter diesen können und wollen wir aber, genau, wie dies a. S. 45 unten für die rationalen Zahlen geschah, nur solche Entwicklungen von $\omega_0, \omega_1, \ldots \omega_{p-2}$ als die p-adischen Reihen für diese algebraischen Zahlen ansehen, für welche jede rationale Gleichung:

$$\varphi(\omega_0,\ \omega_1, \ldots \omega_{p-2}) = 0 \tag{5}$$

mit rationalen Koeffizienten, welche der Größe nach besteht, auch für den Bereich von p richtig bleibt und umgekehrt.

Damit dies der Fall sei, muß zunächst, wenn ω_0 der Größe nach gleich 1 ist, dieselbe Wurzel auch für den Bereich von p gleich 1 sein, da andernfalls die Gleichung $\omega_0 - 1 = 0$ zwar der Größe nach, aber nicht für den Bereich von p erfüllt wäre. Ist zweitens der Größe nach etwa ω_1 gleich der primitiven Wurzel $\bar{\omega}$ in (4a), so muß für den Bereich von p ω_1 gleich einer primitiven Wurzel also etwa gleich ω in (4c) sein; gehörte nämlich ω_1 für den Bereich von p zu einem Teiler d von $p-1$ als Exponenten, so bestünde für den Bereich von p die ganzzahlige Gleichung:

$$\omega_1^d = 1 \qquad (p)$$

während diese der Größe nach nicht erfüllt wäre. Ist endlich die Bezeichnung der Wurzeln $\omega_0, \omega_1, \ldots \omega_{p-2}$ von vornherein so gewählt, daß allgemein der Größe nach

$$\omega_i = \bar{\omega}^i \qquad (i = 0, 1 \cdots p-2)$$

ist, so muß auch für den Bereich von p

$$\omega_i = \omega^i \qquad (i = 0, 1 \cdots p-2)$$

sein, weil andernfalls die ganzzahlige Gleichung

$$\omega_i - \omega_1{}^i = 0$$

der Größe nach, aber nicht für den Bereich von p, erfüllt wäre.

Entwickelt man nun die $p-1$ Wurzeln $(\omega_0, \omega_1, \ldots \omega_{p-1})$ der Kreisteilungsgleichung so, daß allgemein die Gleichungen:

(6) $$\omega_i = \bar{\omega}^i, \qquad \omega_i = \omega^i \quad (p) \qquad (i = 0, 1 \cdots p-2)$$

erfüllt sind, wo $\bar{\omega}$ und ω zwei primitive Wurzeln der Kreisteilungsgleichung der Größe nach und für den Bereich von p bedeuten, so zeigt man jetzt leicht, daß wirklich jede Gleichung (5) dann und nur dann der Größe nach besteht, wenn sie für den Bereich von p erfüllt ist, und umgekehrt.

Wir können zunächst die linke Seite der Gleichung (5) als eine ganze Funktion der ω_i voraussetzen, da wir ja den eventuell auftretenden gemeinsamen Nenner durch Multiplikation fortschaffen können. Besteht nun zwischen den $(p-1)^{\text{ten}}$ Einheitswurzeln ihrer Größe nach eine rationale Gleichung:

(7) $$\varphi(\omega_0, \omega_1, \ldots \omega_{p-2}) = 0$$

mit rationalen Zahlkoeffizienten, und ersetzt man diese Wurzeln ω_i durch ihre Reihenentwicklungen $\bar{\omega}^i$, so geht dieselbe über in:

(7a) $$\varphi(1, \bar{\omega}, \bar{\omega}^2, \ldots \bar{\omega}^{p-2}) = 0.$$

Ist nun wieder

$$g(x) = 0$$

die irreduktible Gleichung (4) a. S. 84, der die primitive Wurzel $\bar{\omega}$ mit ihren $\varphi(p-1)$ konjugierten genügt, so ist die Gleichung (7) dann und nur dann erfüllt, wenn für ein variables x:

(7b) $$\varphi(1, x, \ldots x^{p-2}) = g(x)\,h(x)$$

ist, wo $h(x)$ offenbar ebenfalls eine ganze Funktion von x mit rationalen Zahlkoeffizienten ist. Betrachtet man nun diese Identität (7b) für den Bereich von p, ersetzt x durch die primitive p-adische Wurzel ω und beachtet dabei, daß nach der a. S. 84 gemachten Bemerkung (4a) $g(\omega_1) = 0\ (p)$ ist, so ergibt sich in der Tat:

$$\varphi(1, \omega, \omega^2 \ldots \omega^{p-2}) = 0 \qquad (p),$$

d. h. die Gleichung (7) besteht auch für den Bereich von p.

Besteht umgekehrt die Gleichung (7) für den Bereich von p, und ersetzt man die Wurzeln ω_i durch ihre p-adischen Entwicklungen ω^i, so erhält man die p-adische Gleichung:

$$\varphi(1, \omega, \omega^2, \ldots \omega^{p-2}) = 0 \qquad (p),$$

d. h. die Gleichung mit rationalen Zahlkoeffizienten:

$$\varphi(1, x, \ldots x^{p-2}) = 0 \qquad (p)$$

hat mit der ganzzahligen Gleichung

$$g(x) = 0 \qquad (p)$$

mindestens die eine p-adische Wurzel $x = \omega$ gemeinsam. Daraus folgt, daß die beiden Funktionen $g(x)$ und $\varphi(1, x, \ldots x^{p-2})$ einen

größten gemeinsamen p-adischen Teiler mindestens vom ersten Grade haben müssen, welcher, da er durch das Euklidische Verfahren aus $\varphi(1, x, \ldots x^{p-2})$ und $g(x)$ gefunden werden kann, ebenfalls rationale Zahlkoeffizienten besitzen muß. Da aber $g(x)$ im Körper der rationalen Zahlen irreduktibel ist, also keinen solchen Teiler haben kann, so muß jener Teiler gleich $g(x)$ selber sein, d. h. es besteht wieder eine Identität (7b), und wenn man jetzt in ihr $x = \bar{\omega}$ setzt, so folgt, daß in der Tat auch der Größe nach

$$\varphi(1, \bar{\omega}, .., \bar{\omega}^{p-2}) = 0$$

ist, und damit ist unsere Behauptung vollständig bewiesen.

Aus dem Beweise ergibt sich, daß unserer zweiten a. S. 92 Mitte aufgestellten Forderung dann und nur dann genügt wird, wenn die erste Wurzel ω_1 ihrer Größe nach einer primitiven Gleichungswurzel ω und für den Bereich von p irgend einer p-adischen primitiven Wurzel $\boldsymbol{\omega}$ gleichgesetzt wird. Da es genau $\varphi(p-1)$ solche Zuordnungen gibt, so erhält man also den Satz:

> Man kann die $p-1$ $(p-1)^{\text{ten}}$ Wurzeln der Einheit auf genau $\varphi(p-1)$ verschiedene Arten in p-adische Reihen so entwickeln, daß jede rationale Gleichung mit rationalen Koeffizienten zwischen denselben der Größe nach besteht, welche auch für den Bereich von p gilt und umgekehrt.

Aus dem soeben nur ganz kurz behandelten Beispiele folgt, daß man die Wurzeln der speziellen einfachen Kreisteilungsgleichung (4) so in p-adische Reihen entwickeln kann, daß jede zwischen ihnen bestehende rationale Gleichung auch für den Bereich von p erfüllt ist, und umgekehrt. Ich werde im folgenden zeigen, daß derselbe Fundamentalsatz für alle algebraischen Zahlen gilt. Mit seiner Hilfe können dann die arithmetischen Eigenschaften aller algebraischen Zahlen in wunderbarer Einfachheit und Vollständigkeit ergründet werden, und es wird sich zeigen, daß diese zu den rationalen Zahlen in genau derselben Beziehung stehen, wie die algebraischen Funktionen zu den rationalen Funktionen.

Um aber dieses Resultat ableiten zu können, muß ich zuerst zeigen, daß sich der Bereich der p-adischen Zahlen so erweitern läßt, daß jede algebraische Zahl für den Bereich einer beliebigen Primzahl p einer einzigen p-adischen Zahl dieses erweiterten Bereiches gleich ist. Dieses Resultat soll in den nächsten Kapiteln hergeleitet werden.

Fünftes Kapitel.

Untersuchung der algebraischen Zahlen in bezug auf ihre Größe.

§ 1. Einleitung.

Die am Schlusse des vorigen Kapitels betrachteten Beispiele haben schon gezeigt, daß das große Gebiet der p-adischen Zahlen noch lange nicht dem Anspruche genügt, welchen die Zahlenlehre stellen muß, daß nämlich alle arithmetischen Operationen innerhalb desselben unbeschränkt ausgeführt werden können. Schon die einfache Operation der Wurzelausziehung führte ja im allgemeinen aus dem Bereiche der p-adischen Operationen heraus, denn wir sahen, daß die μ^{te} Wurzel aus einer Zahl B nur unter sehr beschränkenden Voraussetzungen im Gebiete der p-adischen Zahlen existiert. Aber nicht bloß die reinen Gleichungen:

$$x^\mu - B = 0$$

besitzen im Bereiche der p-adischen Zahlen im allgemeinen keine Wurzeln, sondern dasselbe gilt in viel höherem Maße von den algebraischen Gleichungen:

$$B_0 x^\mu + B_1 x^{\mu-1} + \cdots + B_\mu = 0$$

mit beliebigen ganzzahligen Koeffizienten. Bis jetzt ist nur bewiesen worden, daß ihre linken Seiten für den Bereich von p auf eine einzige Weise in irreduktible Faktoren mit p-adischen Koeffizienten zerlegt werden können, aber im allgemeinen sind diese nicht linear, d. h. eine solche Gleichung besitzt im allgemeinen keine p-adischen Wurzeln.

Man kann aber das Gebiet der p-adischen Zahlen in höchst einfacher Weise so erweitern, daß alle für diese geltenden Gesetze in dem größeren Zahlbereiche vollständig unverändert fortbestehen, und daß in diesem jede Funktion μ^{ten} Grades auf eine und nur eine Weise in das Produkt von μ Linearfaktoren zerfällt; aus der dann geltenden Gleichung:

$$F(x) = B_0(x - x_1)(x - x_2) \cdots (x - x_\mu) = 0 \qquad (p)$$

folgt sofort, daß in diesem größeren Gebiete jede Gleichung genau so viele Wurzeln besitzt, als ihr Grad angibt, und daß diese μ allgemeineren p-adischen Zahlen x_i genau dieselben algebraischen Eigenschaften haben, wie die ihrer Größe nach durch reelle oder komplexe Dezimalbrüche dargestellten Gleichungswurzeln.

Im nächsten Kapitel soll diese Erweiterung des Bereiches der p-adischen Zahlen ausführlich dargelegt werden. In dem vorliegenden Kapitel will ich zunächst die algebraischen Zahlen, d. h. die Wurzeln algebraischer Gleichungen in bezug auf ihre Größe untersuchen, ohne sie zu einer bestimmten Primzahl p in Beziehung zu setzen.

§ 2. Die algebraischen Zahlen.

Eine Zahl α, welche ihrer Größe nach einer algebraischen Gleichung:

(1) $$F(x) = x^m + B_1 x^{m-1} + \cdots + B_m = 0$$

mit ganzzahligen oder rational gebrochenen Zahlkoeffizienten genügt, heißt eine algebraische Zahl. Da sich die Wurzeln einer solchen Gleichung nicht ändern, wenn man ihre linke Seite durch eine von Null verschiedene Konstante dividiert, so kann der Koeffizient der höchsten Potenz von x, wie es hier geschehen ist, gleich Eins angenommen werden. Gauß hat zuerst den strengen Beweis erbracht, daß eine jede solche Gleichung im Gebiete der gewöhnlichen komplexen Zahlen genau m Wurzeln besitzt. Bei unseren späteren Untersuchungen wird es sich meistens um ganz einfache Gleichungen, meistens nur um reine Gleichungen

$$x^m - B_0 = 0$$

handeln, deren Wurzeln explizite mittels Wurzelausziehungen dargestellt werden können. Wir wollen aber die folgenden Untersuchungen für die Wurzeln beliebiger Gleichungen durchführen und für sie also den Gaußschen Existenzbeweis als geführt voraussetzen.

Eine algebraische Zahl genügt nicht bloß einer, sondern unendlich vielen Gleichungen. Denn ist $F(\alpha) = 0$ und $G(x)$ eine beliebige andere Funktion von x, so ist ja $x = \alpha$ auch eine Wurzel der Gleichung $H(x) = F(x)\,G(x) = 0$, weil ja $H(\alpha) = F(\alpha)\,G(\alpha) = 0$ ist.

Unter allen Gleichungen, denen eine algebraische Zahl genügt, muß eine existieren, deren Grad möglichst klein ist. Ist

(2) $$f(x) = x^\lambda + a_1 x^{\lambda-1} + \cdots + a_\lambda = 0$$

eine solche Gleichung niedrigsten Grades, so ist sie eindeutig bestimmt, denn gäbe es noch eine andere Gleichung desselben Grades:

$$\bar{f}(x) = x^\lambda + \bar{a}_1 x^{\lambda-1} + \cdots + \bar{a}_\lambda = 0,$$

welche ebenfalls durch α befriedigt wird, so würde ihre Differenz

$$f(x) - \bar{f}(x) = (a_1 - \bar{a}_1)x^{\lambda-1} + \cdots + (a_\lambda - \bar{a}_\lambda) = 0$$

eine Gleichung von niedrigerem als dem λ^{ten} Grade sein, welche ebenfalls durch $x = \alpha$ erfüllt würde, was gegen unsere Voraussetzung verstößt.

Diese Funktion niedrigsten Grades $f(x)$ ist im Bereiche $K(1)$ der rationalen Zahlen irreduktibel, d. h. sie ist nicht gleich dem Produkte $g(x)h(x)$ zweier Funktionen niedrigeren Grades. Wäre nämlich

$$f(x) = g(x)h(x), \qquad \text{also} \qquad f(\alpha) = g(\alpha)h(\alpha) = 0,$$

so würde ja α einer der beiden Gleichungen niedrigeren Grades $g(x) = 0$, oder $h(x) = 0$ genügen. Ist λ der Grad der Gleichung niedrigster Ordnung für α, so nenne ich x *eine algebraische Zahl λ^{ten} Grades.*

Es sei α eine algebraische Zahl λ^{ten} Grades und $f(x) = 0$ die irreduktible Gleichung λ^{ten} Grades, der α genügt; ist dann $F(x) = 0$ irgend eine andere Gleichung für α, so haben die beiden Funktionen $f(x)$ und $F(x)$ sicher den Linearfaktor $(x - \alpha)$ gemeinsam; sie besitzen daher einen größten gemeinsamen Teiler, den man durch das Euklidische Teilerverfahren finden kann. Da aber $f(x)$ irreduktibel ist, so muß dieser Teiler gleich $f(x)$ selber sein. Es besteht somit der Satz:

> Ist α eine algebraische Zahl, welche Wurzel der irreduktiblen Gleichung $f(x) = 0$ ist, so genügt α dann und nur dann einer anderen Gleichung $F(x) = 0$, wenn ihre linke Seite durch $f(x)$ teilbar ist.

Eine jede reduktible oder irreduktible Gleichung m^{ten} Grades besitzt stets m gleiche oder verschiedene Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_m$, und für ein variables x besteht dann die Zerlegung:

$$(3) \qquad F(x) = x^m + B_1 x^{m-1} + \cdots + B_m = (x - \alpha_1) \cdots (x - \alpha_m).$$

Ist $x = \alpha_1$ eine algebraische Zahl λ^{ten} Grades und ist

$$f(x) = x^\lambda + a_1 x^{\lambda-1} + \cdots + a_\lambda = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_\lambda)$$

die Zerlegung der zugehörigen irreduktiblen Gleichung in ihre Linearfaktoren, so sollen $\alpha_1, \alpha_2, \ldots \alpha_\lambda$ die λ zu α_1 *konjugierten algebraischen Zahlen* heißen.

Sind $\alpha_1, \alpha_2, \ldots \alpha_\lambda$ die λ konjugierten Wurzeln einer innerhalb $K(1)$ irreduktiblen Gleichung $f(x) = 0$ und genügt eine unter ihnen, etwa α_1, einer anderen Gleichung $F(x) = 0$, so muß nach dem soeben bewiesenen Satze $F(x) = f(x)g(x)$ sein; ersetzt man in dieser Gleichung x der Reihe nach durch $\alpha_2, \alpha_3, \ldots \alpha_\lambda$, so ergibt sich allgemein

$$F(\alpha_i) = 0 \qquad (i = 1, 2, \cdots \lambda).$$

Eine Gleichung des Bereiches $K(1)$ für eine algebraische Zahl bleibt also richtig, wenn man diese durch ihre λ konjugierten Zahlen ersetzt.

Aus den Elementen der Algebra ergiebt sich endlich der Satz:

Jede symmetrische Funktion der Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_m$ einer Gleichung $F(x) = 0$ ist eine rationale Funktion ihrer Gleichungskoeffizienten $B_1, B_2, \ldots B_m$, also eine rationale Zahl.

§ 3. Die ganzen algebraischen Zahlen.

Eine algebraische Zahl α heißt eine ganze algebraische Zahl, wenn sie irgend einer Gleichung

$$\alpha^m + B_1\alpha^{m-1} + \cdots + B_m = 0 \tag{1}$$

genügt, deren Koeffizienten $B_1, B_2, \cdots B_m$ ganze rationale Zahlen sind.

Diese Definition ist deshalb besonders bequem, weil nach ihr nur eine unter den unendlich vielen Gleichungen für α ganzzahlige Koeffizienten zu haben braucht.

Die ganzen algebraischen Zahlen sind eine Verallgemeinerung der ganzen rationalen Zahlen, denn eine ganze rationale Zahl a genügt ja der linearen Gleichung $x - a = 0$ mit ganzzahligen Koeffizienten. Man kann aber auch den präziseren Satz aussprechen:

Eine ganze algebraische Zahl, die zugleich rational ist, muß eine ganze rationale Zahl sein.

Es sei nämlich α eine ganze algebraische Zahl, und es möge (1) eine ganzzahlige Gleichung sein, welcher α genügt. Weiß man nun ferner, daß $\alpha = \frac{M}{N}$ ein rationaler Bruch ist, dessen Zähler und Nenner teilerfremd sind, so ergibt die Substitution dieses Wertes in (1) eine Gleichung:

$$M^m + B_1 M^{m-1} N + \cdots + B_m N^m = 0. \tag{2}$$

Enthielte nun N auch nur einen Primteiler p, so folgt aus dieser Gleichung, daß derselbe auch in M^m, also auch in M enthalten wäre gegen unsere Voraussetzung; also muß $N = \pm 1$, also $\alpha = \pm M$ eine ganze Zahl sein.

Die ganzen algebraischen Zahlen bilden nun ebenso wie die ganzen rationalen Zahlen einen Bereich, dessen Individuen sich durch die drei elementaren Operationen der Addition, Subtraktion und Multiplikation wieder erzeugen. Es besteht nämlich der Satz:

Sind α und β zwei ganze algebraische Zahlen, so sind auch die drei Zahlen $\alpha + \beta$, $\alpha - \beta$ und $\alpha\beta$ ebenfalls algebraisch ganz.

Es seien nämlich:

$$F(\alpha) = \alpha^m + A_1\alpha^{m-1} + \cdots + A_m = 0,$$

(3) $$G(\beta) = \beta^n + B_1\beta^{n-1} + \cdots\cdots\cdots + B_n = 0$$

die ganzzahligen Gleichungen, denen α und β genügen, und es bedeute

$$\gamma = (\alpha + \beta, \quad \alpha - \beta, \quad \alpha\beta)$$

eine der drei zu untersuchenden Zahlen. Um nun zu beweisen, daß γ ebenfalls einer ganzzahligen Gleichung genügt, setzen wir $mn = r$ und bezeichnen die r Produkte:

(4) $$\alpha^i\beta^k \qquad \begin{pmatrix} i = 0, 1, \cdots m-1 \\ k = 0, 1, \cdots n-1 \end{pmatrix}$$

in irgend einer Reihenfolge mit $\gamma_1, \gamma_2, \ldots \gamma_r$. Bildet man dann die r Produkte:

(5) $$\gamma\gamma_1, \gamma\gamma_2, \cdots \gamma\gamma_r,$$

so sind diese entweder direkt oder mit Hilfe der Gleichungen (3) homogen und linear durch $\gamma_1, \gamma_2, \ldots \gamma_r$ mit ganzzahligen Koeffizienten darstellbar, d. h. es bestehen r Gleichungen von der Form:

(6) $$\begin{aligned} \gamma\gamma_1 &= g_{11}\gamma_1 + g_{12}\gamma_2 + \cdots + g_{1r}\gamma_r, \\ \gamma\gamma_2 &= g_{21}\gamma_1 + g_{22}\gamma_2 + \cdots + g_{2r}\gamma_r, \\ &\vdots \\ \gamma\gamma_r &= g_{r1}\gamma_1 + g_{r2}\gamma_2 + \cdots + g_{rr}\gamma_r, \end{aligned}$$

wo die g_{ik} ganze rationale Zahlen sind. Wenn man also aus diesen r Gleichungen $\gamma_1, \gamma_2, \ldots \gamma_r$ eliminiert, so ergibt sich für γ die Gleichung:

(7) $$\begin{vmatrix} g_{11} - \gamma, & g_{12} & \cdots & g_{1r} \\ g_{21}, & g_{22} - \gamma & \cdots & g_{2r} \\ \vdots & \vdots & & \vdots \\ g_{r1}, & g_{r2} & \cdots & g_{rr} - \gamma \end{vmatrix} = 0,$$

oder entwickelt eine Gleichung:

(7a) $$\gamma^r + G_1\gamma^{r-1} + \cdots + G_r = 0,$$

deren Koeffizienten $G_1, G_2, \ldots G_r$ offenbar ganze rationale Zahlen sind. Damit ist bewiesen, daß γ in der Tat eine ganze algebraische Zahl ist. Aus diesem Satze ergibt sich sofort die Folgerung:

> Jede ganze rationale Funktion $F(\alpha, \beta, \ldots k)$ von beliebig vielen ganzen algebraischen Zahlen mit ganzzahligen Koeffizienten ist wieder eine ganze algebraische Zahl.

Es sei nun α_1 eine ganze algebraische Zahl λ^{ten} Grades, und

(8) $$f(x) = x^\lambda + a_1x^{\lambda-1} + \cdots + a_\lambda = 0$$

sei die irreduktible Gleichung niedrigsten Grades, der α genügt, so könnten diese Koeffizienten gebrochene rationale Zahlen sein, denn zu-

nächst ist ja nur vorausgesetzt, daß eine der unendlich vielen Gleichungen für α ganzzahlige Koeffizienten hat. Aber man beweist jetzt leicht den Satz:

Eine Zahl α ist dann und nur dann algebraisch ganz, wenn die irreduktible Gleichung niedrigsten Grades für α ganzzahlige Koeffizienten hat.

Hat nämlich die Gleichung $f(x) = 0$ ganzzahlige Koeffizienten, so ist α nach unserer Definition algebraisch ganz. Ist umgekehrt α algebraisch ganz, so gibt es eine ganzzahlige Gleichung:

$$(8a) \qquad F(x) = x^m + A_1 x^{m-1} + \cdots + A_m = 0,$$

der α genügt. Dann besitzt also die irreduktible Funktion $f(x)$ mit dieser Funktion $F(x)$ eine gemeinsame Wurzel. Also ist $F(x)$ durch $f(x)$ teilbar, d. h. alle Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_\lambda$ von $f(x) = 0$ sind ganze algebraische Zahlen, da sie auch Wurzeln der Gleichung $F(x) = 0$ sind.

Beachtet man nun, daß die Koeffizienten $a_1, a_2 \ldots a_\lambda$ von $f(x)$ die elementaren symmetrischen Funktionen, also ganze ganzzahlige Funktionen der ganzen algebraischen Zahlen $\alpha_1, \alpha_2, \ldots \alpha_\lambda$ sind, so lehrt unser allgemeiner Satz S. 99 unten, daß auch diese Koeffizienten algebraisch ganz sind; und da sie außerdem rational sind, so müssen sie nach (2) ganze rationale Zahlen sein, w. z. b. w.

Ebenso wie bei den rationalen Zahlen gilt auch hier der Satz:

Jede gebrochene algebraische Zahl läßt sich als Quotient von zwei ganzen algebraischen Zahlen darstellen.

In der Tat, sei β eine gebrochene algebraische Zahl und

$$(9) \qquad \beta^m + B_1 \beta^{m-1} + \cdots + B_m = 0$$

eine Gleichung, der β genügt. Dann sind die Koeffizienten B_i nicht sämtlich ganze Zahlen, und es sei allgemein: $B_i = \frac{b_i}{b_0}$, wo b_0 der Generalnenner der m Zahlen B_i ist. Multipliziert man dann die ganze Gleichung (9) mit b_0^m und schreibt sie in der Form:

$$(9a) \qquad \begin{aligned} &(b_0\beta)^m + B_1 b_0 (b_0\beta)^{m-1} + B_2 b_0^2 (b_0\beta)^{m-2} + \cdots + B_m b_0^m \\ &= (b_0\beta)^m + b_1 (b_0\beta)^{m-1} + b_2 b_0 (b_0\beta)^{m-2} + \cdots + b_m b_0^{m-1} = 0, \end{aligned}$$

so erkennt man, daß die Zahl $\gamma = b_0\beta$ algebraisch ganz ist, da sie der ganzzahligen Gleichung m^{ten} Grades (9a) genügt. Also ist in der Tat:

$$(9b) \qquad \beta = \frac{\gamma}{b_0},$$

und hier sind Zähler und Nenner ganze algebraische Zahlen; das letztere, weil ja b_0 eine rationale ganze Zahl ist.

Endlich werde auch noch der folgende wichtige Satz hervorgehoben, welcher im folgenden häufig angewendet werden wird:

Die Wurzeln einer Gleichung

(10) $$h(\alpha) = \alpha^r + \gamma_1 \alpha^{r-1} + \cdots + \gamma_r = 0$$

von beliebigem Grade, deren Koeffizienten ganze algebraische Zahlen sind, sind selbst ganze algebraische Zahlen.

Zum Beweise denke ich mir alle diejenigen Funktionen

$$h(\alpha),\ h_1(\alpha),\ h_2(\alpha)\ \ldots\ h_{\mu-1}(\alpha)$$

gebildet, welche aus $h(\alpha)$ dadurch hervorgehen, daß die r ganzen algebraischen Zahlen $\gamma_1, \gamma_2, \ldots \gamma_r$ unabhängig voneinander durch ihre Konjugierten $\gamma_1, \gamma_1', \ldots; \gamma_2, \gamma_2', \ldots; \ldots$ ersetzt werden, welche ebenfalls ganze algebraische Zahlen sind. Dann genügt α auch der Gleichung:

(10a) $$H(\alpha) = h(\alpha)\, h_1(\alpha) \ldots h_{\mu-1}(\alpha) = 0,$$

da ihr erster Faktor $h(\alpha) = 0$ ist. Die Koeffizienten von $H(\alpha)$ sind nun reelle ganze Zahlen, da das rechts stehende Produkt eine ganze ganzzahlige Funktion aller konjugierten Zahlen $\gamma_i, \gamma_i', \ldots$ ist, welche in ihnen offenbar symmetrisch ist. Also genügt α auch der Gleichung $H(\alpha) = 0$ mit reellen ganzzahligen Koeffizienten, ist also wirklich algebraisch ganz.

Eine algebraische Zahl α heißt durch eine andere β teilbar, wenn der Quotient $\frac{\alpha}{\beta}$ eine ganze algebraische Zahl ist. Diese Definition der Teilbarkeit stimmt genau mit der entsprechenden für rationale Zahlen überein.

Ist sowohl α durch β als auch umgekehrt β durch α teilbar, so heißen diese beiden Zahlen äquivalent. Sind α und β speziell rationale Zahlen, so sind sie nach dieser Definition offenbar dann und nur dann äquivalent, wenn sie, abgesehen vom Vorzeichen, gleich sind, wenn also $\alpha = \varepsilon\beta$ ist, wo $\varepsilon = \pm 1$ ist.

Setzt man auch in unserem Falle $\frac{\alpha}{\beta} = \varepsilon$, so ist α nur dann äquivalent β, wenn sowohl $\varepsilon = \frac{\alpha}{\beta}$, als $\frac{1}{\varepsilon} = \frac{\beta}{\alpha}$ algebraisch ganz ist.

Eine ganze algebraische Zahl ε, deren reziproker Wert $\frac{1}{\varepsilon}$ wieder ganz ist, heißt eine Einheit. Die algebraischen Einheiten sind die Verallgemeinerung der beiden rationalen Einheiten $+1$ und -1.

Daraus folgt jetzt sofort der Satz:

Zwei Zahlen α und β sind in bezug auf ihre Teilbarkeit dann und nur dann äquivalent, wenn sie sich nur durch

eine Einheit unterscheiden, wenn also $\beta = \alpha\varepsilon$ ist, und ε eine Einheit bedeutet.

Ist

$$f(\varepsilon) = \varepsilon^\lambda + g_1\varepsilon^{\lambda-1} + \cdots + g_\lambda = 0$$

die irreduktible ganzzahlige Gleichung, welcher die Einheit ε genügt, so erkennt man sofort durch Division mit $g_\lambda \varepsilon^\lambda$, daß $\frac{1}{\varepsilon}$ Wurzel der irreduktiblen Gleichung

$$\left(\frac{1}{\varepsilon}\right)^\lambda + \frac{g_{\lambda-1}}{g_\lambda}\left(\frac{1}{\varepsilon}\right)^{\lambda-1} + \cdots + \frac{1}{g_\lambda} = 0$$

ist, und diese ist dann und nur dann ebenfalls ganzzahlig, wenn $g_\lambda = \pm 1$ ist. Es ergibt sich also der Satz:

Eine Zahl ε ist dann und nur dann eine algebraische Einheit, wenn in der zugehörigen ganzzahligen Gleichung niedrigsten Grades das konstante Glied gleich ± 1 ist.

§ 4. Die algebraischen Zahlkörper.

Es sei nun α irgend eine algebraische Zahl, λ sei ihr Grad, und es möge:

(1) $$f(x) = x^\lambda + a_1 x^{\lambda-1} + \cdots + a_\lambda = 0$$

die irreduktible Gleichung des λ^{ten} Grades sein, der α nebst ihren Konjugierten genügt. Im folgenden werden die λ konjugierten Wurzeln der Gleichung (1) durch $\alpha_1, \alpha_2, \ldots \alpha_\lambda$ bezeichnet, und α sei eine beliebige unter diesen Zahlen.

Ich betrachte nun alle diejenigen Zahlen, welche aus α durch die vier elementaren Rechenoperationen, die Addition, Subtraktion, Multiplikation und Division hervorgehen, d. h. die Gesamtheit aller rationalen Funktionen von α

(2) $$\beta = \varphi(\alpha) = \frac{g(\alpha)}{h(\alpha)}$$

mit rationalen Zahlkoeffizienten; die Gesamtheit aller dieser rationalen Funktionen von α nenne ich den durch α konstituierten Zahlkörper und bezeichne ihn durch $K(\alpha)$. Durch die λ konjugierten algebraischen Zahlen $\alpha_1, \alpha_2, \ldots \alpha_\lambda$ werden so die λ konjugierten Körper $K(\alpha_1), K(\alpha_2), \ldots K(\alpha_\lambda)$ konstituiert; ich bezeichne einen beliebigen unter ihnen durch $K(\alpha)$.

Von den Zahlen β in (2) sind nur diejenigen auszuschließen, welche unendlich groß sind; dies würde nur dann der Fall sein, wenn der Nenner $h(\alpha) = 0$ wäre. Nach dem a. S. 97 Mitte bewiesenen Satze ist dies nur dann der Fall, wenn die zugehörige Funktion $h(x)$ durch die irreduktible Funktion $f(x)$ teilbar ist, deren Wurzel α ist.

Ersetzt man in (2) α der Reihe nach durch $\alpha_1, \alpha_2, \dots \alpha_\lambda$, so erhält man die λ algebraischen Zahlen $\beta_1, \beta_2, \dots \beta_\lambda$, wo allgemein

(3) $$\beta_i = \varphi(\alpha_i) \qquad (i = 1, 2, \cdots \lambda)$$

ist. Auch diese sollen die λ zu β **konjugierten Zahlen** heißen; sie gehören den λ konjugierten Körpern $K(\alpha_1), \dots K(\alpha_\lambda)$ an.

Jede symmetrische Funktion

$$S(\beta_1, \beta_2, \dots \beta_\lambda) = S(\varphi(\alpha_1), \varphi(\alpha_2), \dots \varphi(\alpha_\lambda))$$

der λ konjugierten Zahl β_i ist eine rationale Zahl, weil sie auch eine symmetrische Funktion von $\alpha_1, \alpha_2, \dots \alpha_\lambda$ ist.

Hieraus folgt unmittelbar der wichtige Satz:

Jede Zahl $\beta_1 = \varphi(\alpha_1)$ des Körpers $K(\alpha_1)$ genügt nebst ihren Konjugierten einer Gleichung des λ^{ten} Grades

(4) $$g(y) = (y - \beta_1) \cdots (y - \beta_\lambda) = y^\lambda + b_1 y^{\lambda-1} + \cdots + b_\lambda = 0,$$

mit rationalen Zahlkoeffizienten, welche entweder selbst irreduktibel, oder die Potenz einer irreduktiblen Funktion ist.

Der erste Teil unserer Behauptung folgt daraus, daß die Koeffizienten b_i symmetrische Funktionen der konjugierten Zahlen $\beta_1, \beta_2, \dots \beta_\lambda$ sind; der zweite Teil ist eine unmittelbare Folge des weiteren Satzes:

Genügt die algebraische Zahl β_1 irgend einer Gleichung:

$$\bar{g}(y) = 0,$$

so genügen derselben Gleichung alle λ konjugierten Zahlen $\beta_1, \beta_2, \dots \beta_\lambda$.

In der Tat bleibt ja die Gleichung:

$$\bar{g}(\beta_1) = \bar{g}(\varphi(\alpha_1)) = 0$$

nach dem a. S. 98 oben bewiesenen Satze richtig, wenn man α_1 durch $\alpha_2, \dots \alpha_\lambda$ ersetzt, d. h. es ist allgemein $\bar{g}(\beta_i) = 0$, w. z. b. w.

Ist nun die Gleichung λ^{ten} Grades $g(y) = 0$ für β in (4) reduktibel, und sind etwa $\bar{g}(y)$ und $\bar{\bar{g}}(y)$ zwei von den irreduktiblen Faktoren von $g(y)$, so werden die beiden Gleichungen:

$$\bar{g}(y) = 0 \quad \text{und} \quad \bar{\bar{g}}(y) = 0$$

nach dem soeben bewiesenen Satze durch alle konjugierten Zahlen $\beta_1, \beta_2, \dots \beta_\lambda$ befriedigt, da ja jede von ihnen mindestens eine unter diesen Zahlen als Wurzel haben muß. Da somit die beiden irreduktiblen Funktionen $\bar{g}(y)$ und $\bar{\bar{g}}(y)$ einen gemeinsamen Teiler haben, so müssen sie identisch sein. Für eine jede Funktion $g(y)$ besteht also stets eine Zerlegung

$$g(y) = (\bar{g}(y))^\nu = (y - \beta_1)(y - \beta_2) \cdots (y - \beta_\lambda),$$

wo $\bar{g}(y)$ eine irreduktible Funktion mit rationalen Koeffizienten ist.

Es sei nun die zu der algebraischen Zahl β gehörige irreduktible Funktion vom Grade $\bar{\lambda}$ und es seien die λ konjugierten Zahlen β so bezeichnet, daß $\beta_1, \beta_2, \cdots \beta_{\bar{\lambda}}$ die sämtlichen Wurzeln von $\bar{g}(y) = 0$ sind, daß also:

$$\bar{g}(y) = (y - \beta_1)(y - \beta_2) \cdots (y - \beta_{\bar{\lambda}})$$

ist. Dann sind alle diese Wurzeln voneinander verschieden. Denn wären auch nur zwei unter ihnen gleich, besäße also $\bar{g}(y)$ auch nur einen quadratischen Faktor, so hätte ja $\bar{g}(y)$ mit seiner Ableitung $\bar{g}'(y)$ einen gemeinsamen Teiler, wäre also nicht irreduktibel. Andererseits ergibt sich aber aus der Gleichung:

$$g(y) = (\bar{g}(y))^{\nu} = ((y - \beta_1)(y - \beta_2) \cdots (y - \beta_{\bar{\lambda}}))^{\nu},$$

daß dann unter den $\lambda = \nu \bar{\lambda}$ konjugierten Zahlen $\beta_1, \beta_2, \ldots \beta_\lambda$ je ν einander gleich sind. Ferner folgt ohne weiteres der wichtige Satz:

Die Gleichung λ^{ten} Grades für eine Zahl β des Körpers $K(\alpha)$ ist dann und nur dann irreduktibel, wenn die λ konjugierten Zahlen $\beta_1, \beta_2, \ldots \beta_\lambda$ sämtlich voneinander verschieden sind.

Es sei $\beta_1 = \varphi(\alpha_1)$ irgend eine Zahl von $K(\alpha_1)$, und $\beta_2, \beta_3, \ldots \beta_\lambda$ ihre $\lambda - 1$ konjugierten Zahlen, dann wird die rationale Zahl:

$$(5) \qquad n(\beta) = \beta_1 \beta_2 \cdots \beta_\lambda$$

die Norm der Zahl β genannt. Später werden wir dies über alle konjugierten Zahlen β_i erstreckte Produkt auch mitunter die volle Norm von β nennen zum Unterschiede von den Partialnormen, bei welchen das Produkt nur über gewisse unter diesen konjugierten Zahlen erstreckt wird. Ist

$$g(y) = y^\lambda + b_1 y^{\lambda - 1} + \cdots + b_\lambda = 0$$

die Gleichung für β, so ist offenbar

$$n(\beta) = (-1)^\lambda b_\lambda.$$

Sind β und γ zwei Zahlen von $K(\alpha)$, so folgt aus der Definitionsgleichung (5) für $n(\beta)$ sofort die Richtigkeit der beiden Gleichungen:

$$n(\beta \cdot \gamma) = \beta_1 \cdots \beta_\lambda \cdot \gamma_1 \cdots \gamma_\lambda = n(\beta) \cdot n(\gamma),$$

$$n\left(\frac{\beta}{\gamma}\right) = \frac{n(\beta)}{n(\gamma)}.$$

Die Norm eines Produktes ist gleich dem Produkte der Normen der Faktoren. Die Norm eines Quotienten ist gleich dem Quotienten der Normen von Zähler und Nenner.

Ist $\beta = m$ eine rationale Zahl, so sind alle λ konjugierten Zahlen gleich m, d. h. es ist

(5a) $$N(m) = m^\lambda.$$

Ist wieder β_1 eine beliebige Zahl von $K(\alpha_1)$ und sind $\beta_2, \ldots \beta_\lambda$ ihre $\lambda - 1$ Konjugierten, so nenne ich das Produkt

(6) $$\delta(\beta_1) = (\beta_1 - \beta_2) \cdots (\beta_1 - \beta_\lambda)$$

nach Hilbert die Differente von β_1. Auch diese Zahl gehört dem Körper $K(\alpha_1)$ an, weil sie in den konjugierten Zahlen $\beta_2, \cdots \beta_\lambda$ symmetrisch ist. Diese letzte Tatsache folgt auch aus der Gleichung für $\delta(\beta_1)$

(6a) $$\delta(\beta_1) = g'(\beta_1),$$

welche sich ja nach Differentiation der Gleichung (4) unmittelbar ergibt, wenn man $y = \beta_1$ setzt.

Endlich betrachte ich das Produkt

(7) $$d(\beta) = \prod_{i<k} (\beta_i - \beta_k)^2 = (\beta_1 - \beta_2)^2 (\beta_1 - \beta_3)^2 (\beta_2 - \beta_3)^2 \cdots (\beta_{n-1} - \beta_n)^2$$

der quadrierten Wurzeldifferenzen. Diese Zahl heißt die Diskriminante der Zahl β. Sie ist eine rationale Zahl, da sie eine symmetrische Funktion von $\beta_1, \beta_2, \ldots \beta_\lambda$ ist. Bekanntlich läßt sie sich als Determinantenquadrat, nämlich in der Form:

(7a) $$d(\beta) = \begin{vmatrix} 1 & \beta_1 & \beta_1^2 & \ldots & \beta_1^{\lambda-1} \\ 1 & \beta_2 & \beta_2^2 & \ldots & \beta_2^{\lambda-1} \\ \vdots \\ 1 & \beta_\lambda & \beta_\lambda^2 & \ldots & \beta_\lambda^{\lambda-1} \end{vmatrix}^2$$

darstellen. Bildet man endlich die λ konjugierten Differenten $\delta(\beta_1)$, $\delta(\beta_2), \ldots \delta(\beta_\lambda)$, so folgt aus (6) leicht, daß $d(\beta)$ bis auf das Vorzeichen mit dem Produkte derselben übereinstimmt, es ist nämlich offenbar:

(7b) $$d(\beta) = (-1)^{\frac{\lambda(\lambda-1)}{2}} n(\delta(\beta)).$$

Ebenso ist nach (7) und nach Formel (8a) a. S. 61:

(7c) $$d(\beta) = (-1)^{\frac{\lambda(\lambda-1)}{2}} D(g(y)) = (-1)^{\frac{\lambda(\lambda-1)}{2}} R(g(y), g'(y)),$$

d. h. die Diskriminante von β unterscheidet sich von der Diskriminante der Gleichung für β höchstens durch das Vorzeichen. Die Diskriminante $d(\beta)$ ist dann und nur dann Null, wenn unter den konjugierten Zahlen $\beta_1, \beta_2, \ldots \beta_\lambda$ mindestens zwei einander gleich sind.

Die Diskriminante $d(\beta)$ ist also dann und nur dann von Null verschieden, wenn die Gleichung λ^{ten} Grades für β irreduktibel ist.

Jede Zahl γ des Körpers $K(\alpha)$ kann auf eine einzige Weise in der Form

(8) $$\gamma = u_0 + u_1\alpha + \cdots + u_{\lambda-1}\alpha^{\lambda-1}$$

dargestellt werden, wo $u_0, u_1, \ldots u_{\lambda-1}$ rationale Zahlen sind.

Soll nämlich diese Gleichung bestehen, so muß sie nach dem a. S. 98 oben bewiesenen Satze richtig bleiben, wenn man γ und α durch ihre λ konjugierten Werte ersetzt. So ergeben sich zur Bestimmung der unbekannten Koeffizienten $u_0, u_1, \ldots u_{\lambda-1}$ die λ linearen Gleichungen:

(8a) $$\begin{aligned} \gamma_1 &= u_0 + u_1\alpha_1 + \cdots + u_{\lambda-1}\alpha_1^{\lambda-1}, \\ \gamma_2 &= u_0 + u_1\alpha_2 + \cdots + u_{\lambda-1}\alpha_2^{\lambda-1}, \\ &\vdots \\ \gamma_\lambda &= u_0 + u_1\alpha_\lambda + \cdots + u_{\lambda-1}\alpha_\lambda^{\lambda-1}. \end{aligned}$$

Aus ihnen bestimmen sich die Unbekannten u_r eindeutig, sobald die Determinante der Koeffizienten:

(8b) $$|1, \alpha, \alpha^2, \cdots \alpha^{\lambda-1}| = \begin{vmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{\lambda-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{\lambda-1} \\ \vdots \\ 1 & \alpha_\lambda & \alpha_\lambda^2 & \cdots & \alpha_\lambda^{\lambda-1} \end{vmatrix}$$

von Null verschieden ist. Dies ist aber der Fall, da ihr Quadrat nach (7a) gleich $d(\alpha) = \Pi(\alpha_i - \alpha_k)^2$ ist, und die λ Wurzeln α_i voneinander verschieden sind.

Also ergibt sich allgemein für u_r die Gleichung:

(8c) $$u_r = \frac{|1, \alpha_i, \cdots \alpha_i^{r-1}, \gamma_i, \alpha_i^{r+1}, \cdots \alpha_i^{\lambda-1}|}{|1, \alpha_i, \cdots \alpha_i^{r-1}, \alpha_i^r, \alpha_i^{r+1}, \cdots \alpha_i^{\lambda-1}|} \quad \begin{pmatrix} i = 1, 2, \cdots \lambda \\ r = 0, 1, \cdots \lambda - 1 \end{pmatrix},$$

wo die Zählerdeterminante aus der Nennerdeterminante dadurch hervorgeht, daß in der r^{ten} Vertikalreihe die Elemente α_i^r durch γ_i ersetzt werden. Jeder Koeffizient ist also eine rationale Funktion von $\alpha_1, \alpha_2, \ldots \alpha_\lambda$, welche, wie man leicht sieht, in diesen Größen symmetrisch ist, da sie bei jeder Vertauschung irgend zweier Wurzeln ungeändert bleibt. Permutiert man nämlich z. B. α_1 und α_2, so vertauschen sich sowohl im Zähler als im Nenner nur die beiden ersten Horizontalreihen der Determinanten, beide multiplizieren sich also mit (-1), d. h. ihr Quotient bleibt ungeändert. Also sind die durch die Gleichungen (8a) bestimmten Koeffizienten u_i wirklich rationale Zahlen. Daß aber die Darstellung (8) eine eindeutige ist, folgt unmittelbar daraus, daß die Koeffizienten u_i durch die λ Gleichungen (8a) eindeutig bestimmt sind.

Genau dieselbe Überlegung zeigt aber auch, daß jede Zahl γ des Körpers $K(\alpha)$ nicht bloß in der Form (8) durch α, sondern auch in

derselben Weise durch eine beliebige andere Zahl β des Körpers $K(\alpha)$ darstellbar ist, falls nur die λ konjugierten Zahlen $\beta_1, \beta_2, \ldots \beta_\lambda$ voneinander verschieden sind, oder, was dasselbe ist, falls nur die Diskriminante $d(\beta)$ der Zahl β nicht Null ist. Soll es nämlich möglich sein, die Größen $v_0, v_1, \ldots v_{\lambda-1}$ als rationale Zahlen so zu bestimmen, daß

$$\gamma = v_0 + v_1\beta + \cdots + v_{\lambda-1}\beta^{\lambda-1} \tag{9}$$

ist, so muß auch diese Gleichung richtig bleiben, wenn man α, d. h. also β und γ durch ihre λ konjugierten Werte ersetzt. Tut man dies, so erhält man auch hier durch den Übergang zu den konjugierten Zahlen für $v_0, v_1, \ldots v_{\lambda-1}$ die λ linearen Gleichungen:

$$\gamma_k = v_0 + v_1\beta_k + \cdots + v_{\lambda-1}\beta_k^{\lambda-1} \qquad (k = 1, 2, \cdots \lambda), \tag{9a}$$

aus denen sich die Koeffizienten v_i dann und nur dann, und zwar eindeutig, bestimmen, wenn die Determinante

$$|1, \beta, \ldots \beta^{\lambda-1}| = \sqrt{d(\beta)} \gtrless 0 \tag{9b}$$

ist. Ist das der Fall, so zeigt die vorher bei (8c) durchgeführte Betrachtung, daß die aus den Gleichungen (9a) berechneten Größen v_i wirklich rationale Zahlen sind.

Eine Zahl β, deren λ konjugierte sämtlich voneinander verschieden sind, oder, was dasselbe ist, deren Bestimmungsgleichung irreduktibel ist, soll eine primitive Zahl des Körpers $K(\alpha)$ genannt werden. Bei dieser Bezeichnung kann man das erlangte Resultat so aussprechen:

Jede Zahl des Körpers $K(\alpha)$ läßt sich auf eine einzige Weise in der Form:

$$u_0 + u_1\alpha + \cdots + u_{\lambda-1}\alpha^{\lambda-1}$$

mit rationalen Zahlkoeffizienten darstellen. An die Stelle von α kann jede andere primitive Zahl β des Körpers $K(\alpha)$ treten.

Jede primitive oder nicht primitive Zahl β des Körpers $K(\alpha)$ bestimmt einen neuen Körper $K(\beta)$, welcher aus allen rationalen Funktionen von β mit rationalen Zahlkoeffizienten besteht. Ist die irreduktible Gleichung $\bar{g}(y) = 0$ für β vom Grade $\bar{\lambda}$, so ist, wie oben bewiesen wurde, $\bar{\lambda}$ entweder gleich λ oder ein Teiler von λ, je nachdem β eine primitive oder eine nicht primitive Zahl von $K(\alpha)$ ist. Da β, also auch jede rationale Funktion von β, auch eine rationale Funktion von α ist, so gehört jedes Element von $K(\beta)$ auch dem Körper $K(\alpha)$ an. Der Körper $K(\beta)$ ist also ein sog. Teiler oder Teilkörper von $K(\alpha)$.

Ist der Grad $\bar{\lambda}$ von $K(\beta)$ nicht gleich λ, also $\bar{\lambda}$ ein eigentlicher Divisor von λ, so enthält der Körper $K(\beta)$ sicher nicht alle Zahlen

von $K(\alpha)$, denn schon die Zahl α, deren Grad gleich λ ist, kann ja nicht in $K(\beta)$ vorkommen; in diesem Falle heißt $K(\beta)$ ein eigentlicher Teiler von $K(\alpha)$. Ist dagegen $\bar{\lambda} = \lambda$, so folgt aus dem obigen Satze, daß jede Zahl von $K(\alpha)$ auch rational durch β darstellbar, daß also $K(\beta) = K(\alpha)$ ist. Es besteht also der Satz:

Ist β eine Zahl des Körpers $K(\alpha)$, so ist der durch β konstituierte Körper $K(\beta)$ gleich $K(\alpha)$ oder gleich einem eigentlichen Teiler von $K(\alpha)$, je nachdem β eine primitive oder eine nicht primitive Zahl von $K(\alpha)$ ist.

Durch genau dieselben Betrachtungen kommen wir nun zu einer ganz allgemeinen Darstellung aller Zahlen des Körpers $K(\alpha)$. Es seien

(10) $$\beta^{(1)}, \beta^{(2)} \dots \beta^{(\lambda)}$$

irgendwelche λ Zahlen des Körpers $K(\alpha)$ und es mögen allgemein:

(10a) $$\beta_i^{(1)}, \beta_i^{(2)}, \dots \beta_i^{(\lambda)} \qquad (i = 1, 2, \cdots \lambda)$$

die zu ihnen konjugierten Zahlen des Körpers $K(\alpha_i)$, d. h. die Zahlen sein, welche aus den λ Zahlen (10) hervorgehen, wenn man in ihnen α durch α_i ersetzt. Bildet man dann das Determinantenquadrat:

(10b) $$d(\beta^{(1)}, \beta^{(2)}, \dots \beta^{(\lambda)}) = \begin{vmatrix} \beta_1^{(1)}, & \beta_1^{(2)}, & \dots & \beta_1^{(\lambda)} \\ \beta_2^{(1)}, & \beta_2^{(2)}, & \dots & \beta_2^{(\lambda)} \\ \cdot & \cdot & \cdot & \cdot \\ \beta_\lambda^{(1)}, & \beta_\lambda^{(2)}, & \dots & \beta_\lambda^{(\lambda)} \end{vmatrix}^2,$$

so zeigt man genau wie vorher, daß $d(\beta^{(1)}, \dots \beta^{(\lambda)})$ eine symmetrische Funktion von $(\alpha_1, \alpha_2, \dots \alpha_\lambda)$, also eine rationale Zahl ist. Diese Zahl soll die Diskriminante des Systems $(\beta^{(1)}, \dots \beta^{(\lambda)})$ genannt werden. Die vorher betrachtete Diskriminante $d(\beta)$ einer Zahl β ist ein spezieller Fall der hier eingeführten, denn es ist ja offenbar:

(10c) $$d(\beta) = d(1, \beta, \beta^2, \dots \beta^{\lambda-1}).$$

Es gibt sicher Systeme $(\beta^{(1)}, \dots \beta^{(\lambda)})$, deren Diskriminante von Null verschieden ist, z. B. gilt dies ja für jedes System $(1, \beta, \dots \beta^{\lambda-1})$, wenn β eine primitive Zahl des Körpers $K(\alpha)$ ist. Jedes solches System soll eine Basis für den Körper $K(\alpha)$ heißen. Diese Bezeichnung wird durch den folgenden Satz gerechtfertigt, welcher genau ebenso bewiesen wird, wie dies vorher für die spezielle Basis $(1, \beta, \dots \beta^{\lambda-1})$ geschah:

Jede Zahl γ des Bereiches $K(\alpha)$ läßt sich auf eine einzige Weise homogen und linear mit rationalen Koeffizienten durch die Elemente $(\beta^{(1)}, \dots \beta^{(\lambda)})$ einer Basis darstellen.

Bestimmt man nämlich die unbekannten Zahlen $v_1, v_2, \dots v_\lambda$ so, daß die λ linearen Gleichungen:

$$(11)\qquad \gamma_i = v_1\beta_i^{(1)} + v_2\beta_i^{(2)} + \cdots + v_\lambda\beta_i^{(\lambda)} \qquad (i = 1, 2, \cdots \lambda)$$

erfüllt sind, so haben dieselben eine eindeutig bestimmte Lösung, wenn die Determinante

$$(11\mathrm{a})\qquad |\beta_i^{(1)}, \beta_i^{(2)}, \ldots \beta_i^{(\lambda)}| = \sqrt{d(\beta^{(1)}, \ldots \beta^{(\lambda)})} \gtrless 0,$$

wenn also das System $(\beta^{(1)}, \ldots \beta^{(\lambda)})$ eine Basis ist; und in diesem Falle ergeben sich die Koeffizienten

$$(11\mathrm{b})\qquad v_k = \frac{|\beta_i^{(1)}, \ldots \gamma_i, \ldots \beta_i^{(\lambda)}|}{|\beta_i^{(1)}, \ldots \beta_i^{(k)}, \ldots \beta_i^{(\lambda)}|} \qquad (i, k = 1, 2, \cdots \lambda)$$

wieder als symmetrische Funktionen der α_i, d. h. als rationale Zahlen, w. z. b. w.

Es gibt unendlich viele Basen $(\beta^{(1)}, \ldots \beta^{(\lambda)})$ für einen Körper $K(\alpha)$; jedes System $(1, \beta, \ldots \beta^{\lambda-1})$ ist eine solche, falls β eine primitive Zahl des Körpers $K(\alpha)$ ist.

Es sei nun $(\beta^{(1)}, \beta^{(2)}, \ldots \beta^{(\lambda)})$ eine Basis für den Körper $K(\alpha)$ und $(\gamma^{(1)}, \gamma^{(2)}, \ldots \gamma^{(\lambda)})$ sei ein beliebiges System von λ Zahlen desselben Körpers. Dann können die λ Elemente $\gamma^{(i)}$ homogen und linear durch die Basis $(\beta^{(1)}, \ldots \beta^{(\lambda)})$ mit rationalen Koeffizienten dargestellt werden, und diese Darstellungen gelten für alle konjugierten Zahlen $\gamma_\iota^{(1)}, \gamma_\iota^{(2)}, \ldots \gamma_\iota^{(\lambda)}$. So ergeben sich die λ^2 linearen Gleichungen:

$$(12)\qquad \begin{aligned} \gamma_\iota^{(1)} &= c_{11}\beta_\iota^{(1)} + c_{12}\beta_\iota^{(2)} + \cdots + c_{1\lambda}\beta_\iota^{(\lambda)}, \\ \gamma_\iota^{(2)} &= c_{21}\beta_\iota^{(1)} + c_{22}\beta_\iota^{(2)} + \cdots + c_{2\lambda}\beta_\iota^{(\lambda)} \qquad (\iota = 1, 2 \ldots \lambda) \\ &\vdots \\ \gamma_\iota^{(\lambda)} &= c_{\lambda 1}\beta_\iota^{(1)} + c_{\lambda 2}\beta_\iota^{(2)} + \cdots + c_{\lambda\lambda}\beta_\iota^{(\lambda)}. \end{aligned}$$

Hieraus ergibt sich nach dem Multiplikationssatze für Determinanten die folgende wichtige Determinantenrelation:

$$(12\mathrm{a})\qquad \begin{vmatrix} \gamma_1^{(1)}, \gamma_1^{(2)}, \ldots \gamma_1^{(\lambda)} \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ \gamma_\iota^{(1)}, \gamma_\iota^{(2)}, \ldots \gamma_\iota^{(\lambda)} \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ \gamma_\lambda^{(1)}, \gamma_\lambda^{(2)}, \ldots \gamma_{(\lambda)}^{(\lambda)} \end{vmatrix} = \begin{vmatrix} c_{11} & c_{12} \cdots c_{1\lambda} \\ c_{21} & c_{22} \cdots c_{2\lambda} \\ \vdots & \\ \vdots & \\ c_{\lambda 1} & c_{\lambda 2} \cdots c_{\lambda\lambda} \end{vmatrix} \begin{vmatrix} \beta_1^{(1)}, \beta_1^{(2)}, \ldots \beta_1^{(\lambda)} \\ \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot \\ \beta_\iota^{(1)}, \beta_\iota^{(2)}, \ldots \beta_\iota^{(\lambda)} \\ \vdots \\ \beta_\lambda^{(1)}; \beta_\lambda^{(2)}, \ldots \beta_\lambda^{(\lambda)} \end{vmatrix},$$

denn man erhält ja die λ Elemente $\gamma_\iota^{(1)}, \ldots \gamma_\iota^{(\lambda)}$ der ι^{ten} Zeile von $|\gamma_\iota^{(i)}|$, wenn man die λ Elemente $\beta_\iota^{(1)}, \ldots \beta_\iota^{(\lambda)}$ von $|\beta_\iota^{(i)}|$ der Reihe nach mit den entsprechenden Elementen der ersten, zweiten, … λ^{ten} Zeile der Determinante $|c_{ik}|$ multipliziert.

Erhebt man die Gleichung (12a) zum Quadrat und führt wieder

die Diskriminanten der Systeme $(\gamma^{(i)})$ und $(\beta^{(i)})$ ein, so erhält man die Fundamentalgleichung:

$$d(\gamma^{(1)}, \dots \gamma^{(\lambda)}) = |c_{ik}|^2 \cdot d(\beta^{(1)}, \dots \beta^{(\lambda)}). \tag{12b}$$

Geht das System $(\gamma^{(1)}, \dots \gamma^{(\lambda)})$ aus dem Basissystem $(\beta^{(1)}, \dots \beta^{(\lambda)})$ durch eine Substitution mit den rationalen Koeffizienten (c_{ik}) hervor, so ist die Diskriminante desselben gleich derjenigen des Basissystemes multipliziert mit dem Quadrate der Substitutionsdeterminante.

Aus diesem Satze ergibt sich nun eine Reihe wichtiger Folgerungen:

Ein System $(\gamma^{(1)}, \dots \gamma^{(\lambda)})$ von λ algebraischen Zahlen ist dann und nur dann eine Basis für den Körper $K(\alpha)$, wenn es aus einer anderen Basis durch eine Substitution mit nicht verschwindender Determinante hervorgeht.

Denn nur in diesem Falle ist ja $d(\gamma^{(1)}, \dots \gamma^{(\lambda)})$ von Null verschieden.

Zweitens erwähne ich noch den folgenden Satz, welcher aber im folgenden nicht weiter gebraucht werden wird:

Ist das System $(\gamma^{(1)}, \gamma^{(2)}, \dots \gamma^{(\lambda)})$ keine Basis, ist also $d(\gamma^{(1)}, \dots \gamma^{(\lambda)}) = 0$, so sind die λ Zahlen $\gamma^{(1)}, \gamma^{(2)}, \dots \gamma^{(\lambda)}$ rational abhängig, d. h. man kann λ nicht sämtlich verschwindende rationale Zahlen $v_1, v_2, \dots v_\lambda$ so bestimmen, daß die Gleichung besteht:

$$v_1 \gamma^{(1)} + v_1 \gamma^{(2)} + \cdots + v_\lambda \gamma^{(\lambda)} = 0. \tag{13}$$

Es ist also in diesem Falle, wenn z. B. $v_\lambda \gtrless 0$ angenommen wird:

$$\gamma^{(\lambda)} = -\left(\frac{v_1}{v_\lambda}\gamma^{(1)} + \cdots + \frac{v_{\lambda-1}}{v_\lambda}\gamma^{(\lambda-1)}\right), \tag{13a}$$

d. h. mindestens eine jener λ Zahlen ist durch die übrigen homogen und linear darstellbar.

Zum Beweise der Relation (13) drücke ich die Elemente $\gamma^{(i)}$ durch eine Basis $(\beta^{(1)}, \dots \beta^{(\lambda)})$ aus. Sind dann:

$$\gamma^{(i)} = \sum_k c_{ik} \beta^{(k)}$$

jene Gleichungen, so ist $|c_{ik}| = 0$, weil $(\gamma^{(1)}, \dots \gamma^{(\lambda)})$ keine Basis ist. Soll nun die Summe (13)

$$\sum_i v_i \gamma^{(i)} = \sum_i \sum_k c_{ik} v_i \beta^{(k)}$$

gleich Null sein, so müssen die Koeffizienten v_i so gewählt werden, daß alle Koeffizienten von $\beta^{(1)}, \dots \beta^{(\lambda)}$ auf der rechten Seite Null sind. Die so sich ergebenden λ homogenen linearen Gleichungen:

(14) $$\sum_i v_i c_{ik} = 0 \qquad (k = 1, 2, \cdots \lambda)$$

für $v_1, \ldots v_\lambda$ besitzen aber stets mindestens eine Lösung außer der selbstverständlichen $v_1 = v_2 = \ldots = v_\lambda = 0$, weil die Determinante $|c_{ik}|$ Null ist; und damit ist unsere Behauptung bewiesen.

§ 5. Die ganzen algebraischen Zahlen und ihre Darstellung durch ein Fundamentalsystem.

In jedem Körper $K(\alpha)$ bilden die ganzen algebraischen Zahlen einen Teilbereich, deren Individuen sich, wie a. S. 98 unten nachgewiesen war, durch die Operationen der Addition, Subtraktion und Multiplikation wieder erzeugen. Da sich ferner jede gebrochene Zahl von $K(\alpha)$ nach dem a. S. 100 Mitte bewiesenen Satze als Quotient zweier ganzen Zahlen desselben Körpers darstellen läßt, so genügt es, nur die ganzen algebraischen Zahlen von $K(\alpha)$ genauer zu untersuchen.

Ist β irgend eine ganze algebraische Zahl des Bereiches $K(\alpha)$, so ist $n(\beta) = \beta_1 \beta_2 \ldots \beta_\lambda$ eine ganze rationale Zahl, und allgemeiner ist jede ganze ganzzahlige symmetrische Funktion von $\beta_1, \beta_2, \ldots \beta_\lambda$ ebenfalls eine ganze rationale Zahl. Daraus folgt sofort, daß die Diskriminante $d(\beta)$ von β rational und ganz ist, und das gleiche gilt von der Diskriminante $d(\beta^{(1)}, \beta^{(2)}, \ldots \beta^{(\lambda)})$ von irgend welchen ganzen algebraischen Zahlen. Die Diskriminante $d(\beta)$ einer ganzen algebraischen Zahl ist eine von Null verschiedene ganze rationale Zahl oder Null, je nachdem β eine primitive Zahl von $K(\alpha)$ ist oder nicht.

Man kann stets eine primitive ganze algebraische Zahl in dem Körper $K(\alpha)$ finden. Ist nämlich β primitiv, aber nicht ganz, so kann man nach (9b) a. S. 100 β in der Form $\frac{\gamma}{b}$ schreiben, wo γ algebraisch ganz ist und b eine ganze rationale Zahl bedeutet; dann ist $\gamma = b\beta$ eine ganze primitive Zahl, weil die λ konjugierten Zahlen $\gamma_i = b\beta_i$ offenbar alle verschieden sind.

Ehe wir nun die ganzen Zahlen von $K(\alpha)$ genauer untersuchen, wollen wir eine Darstellung aller dieser Zahlen durch eine geeignet gewählte Basis von ganzen algebraischen Zahlen angeben, welche die Grundlage für alle folgenden Untersuchungen bildet.

Es ist sehr leicht, zuerst eine Basis anzugeben, durch welche zwar nicht alle, wohl aber unendlich viele ganze Zahlen von $K(\alpha)$ homogen und linear mit ganzzahligen Koeffizienten dargestellt werden können. Ist nämlich β irgend eine primitive ganze Zahl von $K(\alpha)$, so sind die λ Zahlen

$$1, \beta, \beta^2, \ldots \beta^{\lambda-1}$$

sämtlich algebraisch ganz, und hieraus folgt, daß jede Zahl

$$(1) \qquad \gamma = u_0 + u_1\beta + u_2\beta^2 + \cdots + u_{\lambda-1}\beta^{\lambda-1}$$

sicher algebraisch ganz ist, sobald die λ Koeffizienten $u_0, u_1, \ldots u_{\lambda-1}$ ganze rationale Zahlen sind. Da nun jede Zahl des Körpers $K(\alpha)$ in der Form (1) mit ganzen oder mit gebrochenen rationalen Koeffizienten darstellbar ist, so ist nur noch zu untersuchen, ob es auch ganze algebraische Zahlen γ gibt, welche bei ihrer Darstellung in der Form (1) gebrochene rationale Koeffizienten besitzen. Dies ist nun im allgemeinen stets der Fall, aber man zeigt leicht, daß bei einer solchen ganzen Zahl der Generalnenner der Koeffizienten u_i ein Teiler der Diskriminante $d = d(\beta)$ der algebraischen Zahl β sein muß.

Nach dem a. S. 106 bei (8c) bewiesenen Satze ergeben sich nämlich bei der Darstellung (1) einer beliebigen algebraischen Zahl für die Koeffizienten u_k die Werte:

$$u_k = \frac{|1, \beta_i, \beta_i^2 \cdots \gamma_i \cdots \beta_i^{\lambda-1}|}{|1, \beta_i, \beta_i^2 \cdots \beta_i^k \cdots \beta_i^{\lambda-1}|} = \frac{|1, \beta_i \cdots \gamma_i \cdots \beta_i^{\lambda-1}|\,|1, \beta_i \cdots \beta_i^k \cdots \beta_i^{\lambda-1}|}{|1, \beta_i \cdots \beta_i^k \cdots \beta_i^{\lambda-1}|^2}$$
$$= \frac{v_k}{d},$$

wo die Zähler v_k als symmetrische Funktionen der $(\beta_1, \ldots \beta_\lambda, \gamma_1, \ldots \gamma_\lambda)$ rationale Zahlen, und $d = d(\beta)$ die Diskriminante von β ist. Ist nun speziell die darzustellende Zahl γ ebenso wie β algebraisch ganz, so ist der Zähler v_k als eine ganze ganzzahlige symmetrische Funktion der β_i und γ_i eine ganze rationale Zahl, und man erhält somit wirklich das Resultat:

> Eine Zahl γ des Körpers $K(\alpha)$ kann nur dann algebraisch ganz sein, wenn sie durch die Basis $(1, \beta, \ldots \beta^{\lambda-1})$ in der Form:
>
> $$(1a) \qquad \gamma = \frac{v_0 + v_1\beta + v_2\beta^2 + \cdots + v_{\lambda-1}\beta^{\lambda-1}}{d}$$
>
> darstellbar ist, wo die Koeffizienten v_i ganze rationale Zahlen sind und $d = d(\beta)$ die Diskriminante von β ist.

In dieser Form sind natürlich auch die ganzen Zahlen (1) enthalten; für sie ist eben jeder Koeffizient $v_i = du_i$ durch d teilbar.

Nicht alle in der Form (1a) dargestellten Zahlen sind algebraisch ganz, aber für jede einzelne unter ihnen kann man durch die Bildung der zugehörigen Gleichung entscheiden, ob sie algebraisch ganz ist oder nicht. Diese letzte Untersuchung braucht man nun höchstens für die d^λ algebraischen Zahlen γ durchzuführen, für welche bei ihrer Darstellung

in der Form (1a) alle Koeffizienten v_i nicht negativ und kleiner als d sind. Ist dies nämlich bei einer Zahl γ nicht für alle Koeffizienten der Fall, und schreibt man jeden der λ Koeffizienten v_i in der Form:

$$v_i = du_i + v_i^{(0)},$$

wo $v_i^{(0)}$ der kleinste nicht negative Rest von v_i bei der Division durch d ist, so stellt sich ja γ als die Summe von zwei algebraischen Zahlen

$$\begin{aligned}\gamma &= (u_0 + u_1\beta + \cdots + u_{\lambda-1}\beta^{\lambda-1}) + \frac{v_0^{(0)} + v_1^{(0)}\beta + \cdots + v_{\lambda-1}^{(0)}\beta^{\lambda-1}}{d}\\ &= \overline{\gamma} + \gamma_0\end{aligned}$$

dar, von denen die erste $\overline{\gamma}$ nach (1) sicher algebraisch ganz ist; da sich somit die beiden Zahlen γ und γ_0 um die ganze algebraische Zahl $\overline{\gamma}$ unterscheiden, so ist die eine dann und nur dann algebraisch ganz, wenn es die andere ist.

Um also alle ganzen algebraischen Zahlen des Körpers zu kennen, braucht man nur von einer endlichen Anzahl, nämlich von den d^λ Zahlen

$$\text{(1b)} \qquad \frac{v_0 + v_1\beta + \cdots + v_{\lambda-1}\beta^{\lambda-1}}{d} \qquad (v_i = 0, 1, \cdots d-1)$$

festzustellen, ob sie algebraisch ganz sind oder nicht; dies kann für jede durch die Bildung der zugehörigen Gleichung geschehen. Ich denke mir diese Untersuchung durchgeführt und alle ganzen algebraischen Zahlen der Form (1b) hingeschrieben.

Mit Hilfe dieses Resultates kann man nun stets eine solche Basis von λ ganzen algebraischen Zahlen

$$\beta^{(0)}, \ \beta^{(1)}, \ \ldots \ \beta^{(\lambda-1)}$$

finden, daß alle und nur die ganzen algebraischen Zahlen β des Körpers $K(\alpha)$ in der Form:

$$\beta = u_0\beta^{(0)} + u_1\beta^{(1)} + \cdots + u_{\lambda-1}\beta^{(\lambda-1)}$$

mit ganzzahligen Koeffizienten u_i dargestellt sind.

Zu diesem Zwecke betrachte ich alle diejenigen ganzen algebraischen Zahlen des Körpers $K(\alpha)$, welche bei der Darstellung (1a) durch β ganze Funktionen von einem bestimmten s^{ten} Grade sind, wo s eine der Zahlen $0, 1, 2, \ldots \lambda - 1$ ist, d. h. alle ganzen algebraischen Zahlen $\gamma^{(s)}$ von der Form

$$\text{(1c)} \qquad \gamma^{(s)} = \frac{v_0 + v_1\beta + \cdots + v_s\beta^s}{d}.$$

Unter diesen suche ich diejenige oder eine von denen aus, in welcher der Koeffizient v_s der höchsten Potenz von β positiv und möglichst klein ist. Diese Zahl sei:

(1d) $$\beta^{(s)} = \frac{v_0^{(s)} + v_1^{(s)}\beta + \cdots + v_s^{(s)}\beta^s}{d};$$

sie kann stets gefunden werden, da ja nur diejenigen Zahlen (1b) mit modulo d reduzierten Koeffizienten in Frage kommen, welche in β vom s^{ten} Grade sind. Sollte unter ihnen keine einzige algebraisch ganze vorhanden sein, so würde die Zahl:

$$\beta^s = \frac{0 + 0 \cdot \beta + \cdots + d\beta^s}{d}$$

für $\beta^{(s)}$ zu wählen sein. Dieser kleinste Koeffizient $v_s^{(s)}$ ist also immer eine der Zahlen $1, 2, \ldots d$.

Ist nun $\beta^{(s)}$ die so bestimmte ganze Zahl des s^{ten} Grades, und

$$\gamma^{(s)} = \frac{w_0 + w_1\beta + \cdots + w_s\beta^s}{d}$$

irgend eine andere ganze Zahl s^{ten} Grades, so muß der Koeffizient w_s ein Multiplum des kleinsten Koeffizienten $v_s^{(s)}$ sein. Ist nämlich λ irgend eine ganze rationale Zahl, so ist die Differenz

$$\gamma^{(s)} - \lambda\beta^{(s)} = \frac{(w_0 - \lambda v_0^{(s)}) + (w_1 - \lambda v_1^{(s)})\beta + \cdots + (w_s - \lambda v_s^{(s)})\beta^s}{d}$$

wieder eine ganze algebraische Zahl; sie ist dann und nur dann nicht vom s^{ten} Grade, wenn λ so bestimmt ist, daß $w_s - \lambda v_s^{(s)} = 0$ ist, und dies ist nur dann möglich, wenn w_s ein Vielfaches von $v_s^{(s)}$ ist. Wäre aber w_s nicht durch $v_s^{(s)}$ teilbar, so könnte man λ so bestimmen, daß $w_s - \lambda v_s^{(s)}$ positiv und kleiner als $v_s^{(s)}$ würde, und dann wäre $\gamma^{(s)} - \lambda\beta^{(s)}$ eine ganze algebraische Zahl s^{ten} Grades, für welche der Koeffizient von β^s kleiner wäre als $v_s^{(s)}$, gegen die über $v_s^{(s)}$ gemachte Voraussetzung; daraus folgt die Richtigkeit der über $v_s^{(s)}$ aufgestellten Behauptung.

Es seien nun:

(2) $$\begin{aligned} \beta^{(0)} &= \frac{v_0^{(0)}}{d}, \\ \beta^{(1)} &= \frac{v_0^{(1)} + v_1^{(1)}\beta}{d}, \\ \beta^{(2)} &= \frac{v_0^{(2)} + v_1^{(2)}\beta + v_2^{(2)}\beta^2}{d}, \\ &\cdots\cdots\cdots\cdots \\ \beta^{(\lambda-1)} &= \frac{v_0^{(\lambda-1)} + v_1^{(\lambda-1)}\beta + \cdots + v_{\lambda-1}^{(\lambda-1)}\beta^{\lambda-1}}{d} \end{aligned}$$

ein vollständiges System von ganzen algebraischen Zahlen nullten, ersten, ... $(\lambda-1)^{\text{ten}}$ Grades, in deren jeder der Koeffizient der höchsten Potenz von β positiv und möglichst klein ist. Dann bilden die Zahlen $(\beta^{(0)}, \beta^{(1)}, \ldots \beta^{(\lambda-1)})$ eine solche Basis für den Körper $K(\alpha)$, daß alle

und nur die ganzen algebraischen Zahlen desselben auf eine einzige Weise in der Form:

(3) $$u_0\beta^{(0)} + u_1\beta^{(1)} + \cdots + u_{\lambda-1}\beta^{(\lambda-1)}$$

mit **ganzzahligen** Koeffizienten dargestellt sind.

In der Tat, sei

$$\gamma = \frac{v_0 + v_1\beta + \cdots + v_{\lambda-1}\beta^{\lambda-1}}{d}$$

irgend eine ganze algebraische Zahl von $K(\alpha)$, so muß $v_{\lambda-1}$ nach dem soeben geführten Beweise ein Multiplum von $v_{\lambda-1}^{(\lambda-1)}$ sein. Ist nun $v_{\lambda-1} = u_{\lambda-1} v_{\lambda-1}^{(\lambda-1)}$, so ist die Differenz:

$$\gamma - u_{\lambda-1}\beta^{(\lambda-1)} = \frac{v_0' + v_1'\beta + \cdots + v_{\lambda-2}'\beta^{\lambda-2}}{d}$$

eine ganze algebraische Zahl vom $(\lambda-2)^{\text{ten}}$ oder einem niedrigeren Grade in β, weil der Koeffizient von $\beta^{\lambda-1}$ gleich Null wird. Nach demselben Satze ist also jetzt: $v_{\lambda-2}' = u_{\lambda-2} v_{\lambda-2}^{(\lambda-2)}$ ein ganzzahliges Multiplum von $v_{\lambda-2}^{(\lambda-2)}$; es wird also $\gamma - (u_{\lambda-1}\beta^{(\lambda-1)} + u_{\lambda-2}\beta^{(\lambda-2)})$ wieder eine ganze algebraische Zahl sein, welche jetzt höchstens vom $(\lambda-3)^{\text{ten}}$ Grade in β ist, usw. Durch Fortsetzung desselben Verfahrens ergibt sich zuletzt, daß die Differenz:

$$\gamma - (u_{\lambda-1}\beta^{(\lambda-1)} + \cdots + u_1\beta^{(1)} + u_0\beta^{(0)}) = 0$$

ist, wo die u_i lauter ganze Zahlen sind; und damit ist bewiesen, daß jede ganze Zahl γ in der Form (3) mit ganzzahligen Koeffizienten darstellbar ist.

Die λ ganzen Zahlen $(\beta^{(0)}, \beta^{(1)}, \ldots \beta^{(\lambda-1)})$ in (2) bilden auch eine Basis für den Körper $K(\alpha)$, denn sie ergeben sich aus der Basis $(1, \beta, \beta^2, \ldots \beta^{\lambda-1})$ durch die Substitution (2) mit der Determinante:

(4) $$\begin{vmatrix} \frac{v_0^{(0)}}{d}, & 0, & 0, & \cdots & 0 \\ \frac{v_0^{(1)}}{d}, & \frac{v_1^{(1)}}{d}, & 0, & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \frac{v_0^{(\lambda-1)}}{d}, & \frac{v_1^{(\lambda-1)}}{d}, & & \cdots & \frac{v_{\lambda-1}^{(\lambda-1)}}{d} \end{vmatrix} = \frac{v_0^{(0)} v_1^{(1)} \cdots v_{\lambda-1}^{(\lambda-1)}}{d^\lambda},$$

welche sicher von Null verschieden ist. Damit ist unsere Behauptung in allen ihren Teilen erwiesen.

Eine Basis von λ ganzen algebraischen Zahlen $(\gamma^{(1)}, \gamma^{(2)}, \cdots \gamma^{(\lambda)})$ durch welche alle ganzen Zahlen von $K(\alpha)$ auf eine einzige Weise in der Form

$$u_1 \gamma^{(1)} + u_2 \gamma^{(2)} + \cdots + u_\lambda \gamma^{(\lambda)}$$

mit ganzzahligen rationalen Koeffizienten u_i darstellbar sind, soll **ein Fundamentalsystem** für diesen Körper heißen.

Wir haben bewiesen, daß für jeden Körper $K(\alpha)$ **ein** Fundamentalsystem existiert, nämlich das System $(\beta^{(0)}, \beta^{(1)}, \cdots \beta^{(\lambda-1)})$ in (2). Man kann jetzt leicht zeigen, daß aus einem solchen Systeme unendlich viele Fundamentalsysteme hergeleitet werden können. Es besteht nämlich der folgende Satz:

Ist $(\gamma^{(1)}, \gamma^{(2)}, \ldots \gamma^{(\lambda)})$ ein Fundamentalsystem, so geht jedes andere Fundamentalsystem $(\delta^{(1)}, \delta^{(2)}, \ldots \delta^{(\lambda)})$ aus diesem durch eine ganzzahlige Substitution

$$\delta^{(i)} = \sum_k c_{ik} \gamma^{(k)} \qquad (i = 1, 2, \cdots \lambda) \tag{5}$$

hervor, deren Determinante $|c_{ik}| = \pm 1$ ist.

Ist nämlich $(\gamma^{(1)}, \gamma^{(2)}, \ldots \gamma^{(\lambda)})$ ein Fundamentalsystem für $K(\alpha)$ und $(\delta^{(1)}, \delta^{(2)}, \ldots \delta^{(\lambda)})$ irgend ein ganzzahliges System, so sind alle Elemente $\delta^{(i)}$ durch das System $(\gamma^{(1)}, \ldots \gamma^{(\lambda)})$ ganzzahlig darstellbar; es bestehen also die λ ganzzahligen linearen Gleichungen:

$$\delta^{(i)} = \sum_{k=1}^{\lambda} c_{ik} \gamma^{(k)}. \qquad (i = 1, 2, \cdots \lambda)$$

Ist die Substitutionsdeterminante $|c_{ik}| = 0$, so ist auch

$$d(\delta^{(1)}, \ldots \delta^{(\lambda)}) = |c_{ik}|^2 d(\gamma^{(1)}, \ldots \gamma^{(\lambda)}) = 0, \tag{5a}$$

also ist dann das zweite System keine Basis für $K(\alpha)$. Ist aber $|c_{ik}| \gtrless 0$, so ergibt die Auflösung der obigen Gleichungen:

$$\gamma^{(i)} = \sum_{k=1}^{\lambda} c'_{ik} \delta^{(k)}, \qquad (i = 1, 2, \cdots \lambda) \tag{5b}$$

wo die Zahlen c'_{ik} die Elemente des zu (c_{ik}) reziproken Systems sind; sie sind bekanntlich gleich den bezüglichen Unterdeterminanten $(\lambda-1)^{\text{ter}}$ Ordnung der c_{ik}, dividiert durch die Determinante $|c_{ik}|$. Ist nun

$$|c_{ik}| = \pm 1,$$

so sind auch alle Elemente c'_{ik} ganze Zahlen; also sind die λ Zahlen $\gamma^{(i)}$ ganzzahlig durch $(\delta^{(1)}, \ldots \delta^{(\lambda)})$ darstellbar, und somit ist auch jede ganze algebraische Zahl $(u_1 \gamma^{(1)} + \cdots + u_\lambda \gamma^{(\lambda)})$ mit ganzzahligen Koeffizienten

eine ganzzahlige lineare Funktion der $(\delta^{(k)})$. Ist dagegen der gemeinsame Nenner $|c_{ik}|$ von allen c'_{ik} seinem absoluten Werte nach größer als Eins, so können nicht alle Elemente c'_{ik} in (5b) ganze Zahlen sein, denn sonst müßte ja ihre Determinante $|c'_{ik}|$ auch ganz sein und da bekanntlich $|c'_{ik}| = \frac{1}{|c_{ik}|}$ ist, so ist dies dann und nur dann der Fall, wenn $|c_{ik}| = \pm 1$ ist. Nur in diesem Falle sind also die Elemente $\gamma^{(\lambda)}$ und somit auch alle ganzen Zahlen von $K(\alpha)$ ganzzahlig durch das System $(\delta^{(1)}, \dots \delta^{(\lambda)})$ darstellbar, und unsere Behauptung ist daher bewiesen.

Ist $(\delta^{(1)}, \delta^{(2)}, \dots \delta^{(\lambda)})$ irgend ein ganzzahliges System von $K(\alpha)$ und $(\gamma^{(1)}, \gamma^{(2)}, \dots \gamma^{(\lambda)})$ ein Fundamentalsystem, so ist nach (12a) a. S. 109:

$$(6) \qquad d(\delta^{(1)}, \delta^{(2)}, \dots \delta^{(\lambda)}) = |c_{ik}|^2 d(\gamma^{(1)}, \gamma^{(2)}, \dots \gamma^{(\lambda)}),$$

wenn wieder $|c_{ik}|$ die Substitutionsdeterminante der Gleichungen (5) bedeutet. Da diese Determinante stets eine ganze Zahl und dann und nur dann gleich ± 1 ist, wenn auch $(\delta^{(1)}, \dots \delta^{(\lambda)})$ ein Fundamentalsystem ist, so ist stets $|d(\delta^{(i)})| \geqq |d(\gamma^{(i)})|$, und es ergibt sich somit der Satz:

> Ein System ganzer algebraischer Zahlen $(\gamma^{(1)}, \dots \gamma^{(\lambda)})$ ist dann und nur dann ein Fundamentalsystem, wenn seine Diskriminante absolut genommen den kleinstmöglichen Wert hat. Die Diskriminante eines Fundamentalsystems soll die **Körperdiskriminante** genannt werden.

Aus der Gleichung (6) folgt endlich ohne weiteres:

> Die Körperdiskriminante ist der größte gemeinsame Teiler der Diskriminanten $d(\delta^{(1)}, \dots \delta^{(\lambda)})$ aller ganzzahligen Systeme des Körpers $K(\alpha)$. Speziell ist sie also auch ein gemeinsamer Teiler der Diskriminanten $d(\beta) = d(1, \beta, \cdots \beta^{\lambda-1})$ aller ganzen Zahlen des Körpers.

Da die Diskriminanten $d(\beta)$ nach (7c) a. S. 105 mit den Gleichungsdiskriminanten für die ganzen Zahlen β bis auf das Vorzeichen übereinstimmen, so ist die Körperdiskriminante auch **ein** gemeinsamer Teiler der Diskriminanten aller Gleichungen, welchen die ganzen algebraischen Zahlen von $K(\alpha)$ genügen. Es wird sich aber zeigen, daß sie nicht der **größte** gemeinsame Teiler derselben ist, sondern daß alle Gleichungsdiskriminanten außer der Körperdiskriminante, dem s. g. **wesentlichen Teiler**, im allgemeinen noch einen anderen, den s. g. **außerwesentlichen** gemeinsamen Teiler besitzen, dessen vollständige Bestimmung früher sehr erhebliche Schwierigkeiten bereitete. Mit den hier eingeführten Methoden wird die vollständige Bestimmung auch dieser außerwesentlichen Teiler im folgenden höchst einfach ausgeführt werden.

Sechstes Kapitel.

Untersuchung der algebraischen Zahlen für den Bereich einer beliebigen Primzahl. Die p-adischen algebraischen Zahlen.

---

§ 1. Die modulo p ganzen algebraischen Zahlen; ihre Darstellung durch ein Fundamentalsystem.

Ich will jetzt die Zahlen eines algebraischen Körpers $K(\alpha)$ genau ebenso für den Bereich einer beliebigen Primzahl p untersuchen, wie dies im ersten Kapitel für die Zahlen des Körpers $K(1)$ d. h. für die rationalen Zahlen durchgeführt wurde.

Eine rationale Zahl $a = \frac{m}{n}$ des Körpers $K(1)$ wurde „modulo p ganz" genannt, wenn ihr Nenner n durch p nicht teilbar ist, falls jener Bruch in seiner reduzierten Form geschrieben angenommen wird. Wir wollen diesen Begriff für die algebraischen Zahlen folgendermaßen verallgemeinern:

Eine algebraische Zahl β heißt „modulo p ganz", wenn sie mindestens einer Gleichung:

$$\beta^m + B_1\beta^{m-1} + \cdots + B_m = 0 \tag{1}$$

mit modulo p ganzen rationalen Koffizienten genügt, sie heißt „absolut ganz" (vgl. S. 98 (1)), wenn jene Koeffizienten B_i überhaupt keinen Nenner haben. Speziell sind also die modulo p ganzen rationalen Zahlen auch für diese Primzahl algebraisch ganz.

Ist eine algebraische Zahl absolut ganz, so ist sie in bezug auf jede Primzahl p eine ganze algebraische Zahl, aber das Umgekehrte ist offenbar nicht der Fall, denn die Gleichung (1), welcher eine modulo p ganze Zahl genügt, kann sehr wohl gebrochene Koeffizienten haben, nur dürfen die Nenner nicht durch p teilbar sein. Der Bereich aller modulo p ganzen algebraischen Zahlen enthält also den der absolut ganzen Zahlen als Teilbereich, und für diesen größeren Bereich gelten

alle diejenigen Sätze und Beweise, welche wir im § 3 des fünften Kapitels für die absolut ganzen algebraischen Zahlen gefunden hatten. Es mögen diese daher hier nur noch einmal kurz angegeben werden.

I) Eine modulo p ganze algebraische Zahl, welche zugleich rational ist, muß eine modulo p ganze rationale Zahl sein.

Genügt nämlich der rationale reduzierte Bruch $\beta = \frac{M}{N}$ der Gleichung (1) mit modulo p ganzen Koeffizienten, so folgt wieder durch Substitution von β die Gleichung:

$$M^m + B_1 M^{m-1} N + \cdots + B_m N^m = 0, \tag{2}$$

und aus ihr ergibt sich, daß der Nenner N die Primzahl p nicht enthalten kann, da sonst M^m also auch M selbst durch p teilbar sein müßte, während doch M und N teilerfremd sind.

II) Sind α und β zwei modulo p ganze algebraische Zahlen, so sind auch die Zahlen $\alpha + \beta$, $\alpha - \beta$ und $\alpha\beta$ modulo p algebraisch ganz.

Der Beweis wird wörtlich ebenso wie a. S. 99 geführt. Ebenso wie a. S. 100 ergibt sich als unmittelbare Folgerung aus II) der weitere Satz:

III) Eine Zahl β ist dann und nur dann modulo p algebraisch ganz, wenn die (irreduktible) Gleichung **niedrigsten Grades**, der β genügt, modulo p ganzzahlige Koeffizienten hat.

IV) Jede modulo p gebrochene Zahl β läßt sich in der Form

$$\beta = \frac{\gamma}{p^\varrho} \tag{3}$$

darstellen, wo der Zähler γ modulo p ganz ist und p^ϱ eine Potenz von p mit positivem ganzzahligen Exponenten bedeutet.

Ist nämlich β eine modulo p gebrochene algebraische Zahl, und

$$\beta^m + B_1\beta^{m-1} + \cdots + B_m = 0 \tag{4}$$

eine der Gleichungen, welcher β genügt, so sind sicher nicht alle Koeffizienten B_i modulo p ganz. Schreibt man dann diese Koeffizienten B_i in der Form:

$$B_i = \frac{b_i}{p^\varrho}, \tag{5}$$

wo jetzt alle b_i modulo p ganz sind, so zeigt man genau wie a. S. 100, daß die algebraische Zahl $\gamma = p^\varrho \beta$ modulo p ganz, daß also wirklich β in der Form (3) darstellbar ist.

Endlich werde noch der folgende Satz erwähnt, welcher genau wie der entsprechende a. S. 101 oben bewiesen wird:

V) Die Wurzeln einer Gleichung:

$$\alpha^r + \gamma_1 \alpha^{r-1} + \cdots + \gamma_r = 0,$$

deren Koeffizienten modulo p ganze algebraische Zahlen sind, sind selbst modulo p ganze algebraische Zahlen.

Ist der Quotient $\frac{\alpha}{\beta} = \gamma$ zweier Zahlen modulo p algebraisch ganz, so heißt die Zahl α für den Bereich von p durch β teilbar.

Ich betrachte nun die Zahlen eines Körpers $K(\alpha)$ vom λ^{ten} Grade und suche die modulo p ganzen Zahlen desselben durch ein sog. „Fundamentalsystem modulo p" darzustellen. Auch die modulo p ganzen Zahlen von $K(\alpha)$ bilden einen Teilbereich dieses Körpers, dessen Individuen sich nach II. durch Addition, Subtraktion und Multiplikation wiedererzeugen. Sind also $(\gamma^{(1)}, \gamma^{(2)}, \dots \gamma^{(\lambda)})$ λ modulo p ganze algebraische Zahlen, welche eine Basis für den Körper $K(\alpha)$ bilden, so ist jede Zahl γ des Körpers auf eine einzige Weise in der Form

$$\gamma = u_1 \gamma^{(1)} + u_2 \gamma^{(2)} + \cdots + u_\lambda \gamma^{(\lambda)} \tag{6}$$

darstellbar. Sind die Koeffizienten u_i modulo p ganze rationale Zahlen, so ist γ modulo p algebraisch ganz; es könnte aber γ auch für p algebraisch ganz sein, wenn die Zahlen u_i modulo p gebrochen sind. Jedoch kann man die Basis $(\gamma^{(1)}, \dots \gamma^{(\lambda)})$ auch hier stets so wählen, daß diese zweite Eventualität nicht eintreten kann.

Ist die Zahl γ modulo p ganz, so lehrt die Form der a. S. 109 (11b) für die Koeffizienten u_i gefundenen Ausdrücke wieder, daß diese höchstens den gemeinsamen Nenner $d(\gamma^{(1)}, \gamma^{(2)}, \dots \gamma^{(\lambda)})$ haben können, d. h. daß die modulo p ganzen algebraischen Zahlen in der Form darstellbar sind

$$\frac{v_1 \gamma^{(1)} + v_2 \gamma^{(2)} + \cdots + v_\lambda \gamma^{(\lambda)}}{d}, \tag{7}$$

wo die v_i modulo p ganze rationale Zahlen bedeuten und $d = d(\gamma^{(i)})$ ist. Ist also speziell d durch p nicht teilbar, d. h. eine Einheit modulo p, so sind auch die Zahlen $\frac{v_i}{d}$ modulo p ganz, und es ergibt sich so der spezielle Satz:

VI) Jedes System $(\gamma^{(1)}, \gamma^{(2)}, \dots \gamma^{(\lambda)})$ von modulo p ganzen algebraischen Zahlen, dessen Diskriminante $d(\gamma^{(1)}, \dots \gamma^{(\lambda)})$ durch p nicht teilbar ist, ist ein Fundamentalsystem für die modulo p ganzen algebraischen Zahlen.

Ist speziell β eine modulo p ganze algebraische Zahl, deren Diskriminante $d(\beta) = d(1, \beta, \dots \beta^{\lambda-1})$ durch p nicht teilbar ist, so bilden die λ Zahlen $(1, \beta, \dots \beta^{\lambda-1})$ ein solches Fundamentalsystem modulo p, d. h. es besteht der Satz:

VII) Ist β eine modulo p ganze Zahl von $K(\alpha)$, deren Diskriminante p nicht enthält, so sind alle modulo p ganzen algebraischen Zahlen und nur sie in der Form:

$$u_0 + u_1\beta + \cdots + u_{\lambda-1}\beta^{\lambda-1}$$

mit modulo p ganzen rationalen Koeffizienten auf eine einzige Art darstellbar.

Wir werden aber sehr bald zeigen, daß für gewisse Primzahlen p eben eine solche ganze Zahl β in dem Bereiche $K(\alpha)$ nicht existiert, daß sogar allgemeiner jede Diskriminante $d(\gamma^{(1)}, \ldots \gamma^{(\lambda)})$ von irgendwelchen modulo p ganzen Zahlen durch p teilbar ist. Auch in diesem Falle kann man durch die Anwendung der a. S. 113 auseinandergesetzten Methode stets ein Fundamentalsystem modulo p erhalten. Man kann aber hierzu auch jedes absolute Fundamentalsystem gebrauchen. Es gilt nämlich der Satz:

VIII) Jedes absolute Fundamentalsystem ist auch ein Fundamentalsystem für eine beliebige Primzahl p.

Ist nämlich $(\gamma^{(1)}, \gamma^{(2)} \ldots \gamma^{(\lambda)})$ ein absolutes Fundamentalsystem, so sind ja seine Elemente auch modulo p ganze Zahlen, und daher ist zunächst auch jede Zahl

$$\gamma = u_1\gamma^{(1)} + u_2\gamma^{(2)} + \cdots + u_\lambda\gamma^{(\lambda)}$$

modulo p ganz, wenn die Koeffizienten u_i modulo p ganze rationale Zahlen sind.

Dagegen zeigt man leicht, daß eine Zahl

$$\delta = \frac{v_1\gamma^{(1)} + v_2\gamma^{(2)} + \cdots + v_\lambda\gamma^{(\lambda)}}{p}$$

mit modulo p ganzen Koeffizienten v_i, welche auch nur die erste Potenz von p im Nenner hat, nur dann ganz sein kann, wenn alle Koeffizienten v_i durch p teilbar sind, wenn sich also p einfach forthebt. Ist nämlich v_i irgend eine der λ rationalen, aber modulo p ganzen Zahlen, so kann man sie in der Form schreiben:

$$v_i = v_i^{(0)} + p\bar{v}_i, \qquad (i = 1, 2, \cdots \lambda)$$

wo $v_i^{(0)}$ der kleinste ganzzahlige positive Rest von v_i modulo p, also eine der p ganzen Zahlen $0, 1, \ldots p-1$, und $\bar{v}_i = v_i - v_i^{(0)}$ ein modulo p ganzer rationaler Bruch ist. Setzt man diese Werte für die v_i ein, so ergibt sich für die Zahl δ die Zerlegung:

$$\begin{aligned}\delta &= \frac{v_1^{(0)}\gamma^{(1)} + \cdots + v_\lambda^{(0)}\gamma^{(\lambda)}}{p} + \bar{v}_1\gamma^{(1)} + \cdots + \bar{v}_\lambda\gamma^{(\lambda)} \\ &= \delta^{(0)} + \bar{\delta},\end{aligned}$$

und hier ist $\bar{\delta}$, wie soeben gezeigt wurde, modulo p ganz; da sich somit die beiden Zahlen δ und $\delta^{(0)}$ um die modulo p ganze Zahl $\bar{\delta}$ unterscheiden, so sind sie entweder beide ganz oder beide gebrochen modulo p. Aber die reduzierte Zahl

$$\delta^{(0)} = \frac{v_1^{(0)}\gamma^{(1)} + \cdots + v_\lambda^{(0)}\gamma^{(\lambda)}}{p}$$

mit den absolut ganzen Koeffizienten $v_i^{(0)}$ kann nur dann modulo p ganz sein, wenn alle ihre Koeffizienten gleich Null sind. Ist dies nämlich nicht der Fall, so ist $\delta^{(0)}$ nicht absolut ganz, weil $(\gamma^{(1)}, \ldots \gamma^{(\lambda)})$ ein absolutes Fundamentalsystem ist; also müssen die Koeffizienten der Gleichung für $\delta^{(0)}$ mindestens einen Nenner haben, und dieser kann wegen der Form von $\delta^{(0)}$ kein anderer als p sein. Also ist $\delta^{(0)}$ nur dann modulo p ganz, wenn $\delta^{(0)} = 0$, wenn also $\delta = \bar{\delta}$ ist; und damit ist unser Beweis geführt.

Es ist somit bewiesen, daß man in jedem Körper $K(\alpha)$ für eine beliebige Primzahl p ein Fundamentalsystem $(\gamma^{(1)}, \gamma^{(2)}, \ldots \gamma^{(\lambda)})$ finden kann. Ist $(\delta^{(1)}, \delta^{(2)}, \ldots \delta^{(\lambda)})$ wieder irgend ein anderes System modulo p ganzer Zahlen, so hängt dieses mit dem Fundamentalsysteme $(\gamma^{(1)}, \ldots \gamma^{(\lambda)})$ durch eine rationale Substitution:

$$\delta^{(i)} = \sum_k c_{ik}\gamma^{(k)} \qquad (i = 1, 2, \cdots \lambda) \tag{8}$$

zusammen, deren Koeffizienten jetzt nicht mehr absolut ganze Zahlen zu sein brauchen, wohl aber modulo p ganze rationale Zahlen sein müssen, weil $(\gamma^{(1)}, \ldots \gamma^{(\lambda)})$ ein Fundamentalsystem modulo p ist.

Die Determinante $|c_{ik}|$ ist also auch eine modulo p ganze rationale Zahl, und aus der Auflösung der λ Gleichungen (8)

$$\gamma^{(i)} = \sum_k c'_{ik}\,\delta^{(k)}, \qquad (i = 1, 2, \cdots \lambda) \tag{8a}$$

wo die c'_{ik} wieder die Elemente des reziproken Systems zu (c_{ik}) sind, ergibt sich genau wie a. S. 116 der Satz:

> IX) Ist $(\gamma^{(1)}, \gamma^{(2)}, \ldots \gamma^{(\lambda)})$ irgend ein Fundamentalsystem modulo p, so geht jedes andere Fundamentalsystem für dieselbe Primzahl aus diesem durch eine lineare Substitution mit modulo p ganzen Koeffizienten
>
> $$\delta^{(i)} = \sum_k c_{ik}\gamma^{(k)}$$
>
> hervor, deren Determinante $|c_{ik}|$ eine Einheit modulo p ist.

Aus der Gleichung (6) a. S. 117 ergibt sich genau wie a. a. O. der Satz:

> X) Ein System modulo p ganzer algebraischer Zahlen ist dann und nur dann ein Fundamentalsystem modulo p, wenn seine Diskriminante durch eine möglichst niedrige Potenz dieser

Primzahl teilbar ist; sie ist also der größte gemeinsame Teiler modulo p der Diskriminanten von allen modulo p ganzzahligen Systemen $(\delta^{(1)}, \delta^{(2)}, \ldots \delta^{(\lambda)})$.

§ 2. Die Darstellung der Zahlen des Körpers $K(\alpha)$ für den Bereich von p. Die Zahlen des Bereiches $K(p, \alpha)$.

Es sei jetzt

(1) $$\gamma^{(1)}, \gamma^{(2)}, \ldots \gamma^{(\lambda)}$$

irgend ein Fundamentalsystem von $K(\alpha)$ für den Bereich von p. Dann gilt der folgende einfache Satz über die Bedingungen für die Teilbarkeit einer Zahl durch eine Potenz von p mit ganzzahligem Exponenten:

Eine Zahl

(2) $$\gamma = u_1\gamma^{(1)} + u_2\gamma^{(2)} + \cdots + u_\lambda\gamma^{(\lambda)}$$

ist dann und nur dann durch eine ganzzahlige Potenz p^δ von p algebraisch teilbar, wenn alle ihre Koeffizienten u_i durch p^δ teilbar sind.

Soll nämlich $\gamma = p^\delta\bar{\gamma}$ sein, wo $\bar{\gamma} = \bar{u}_1\gamma^{(1)} + \cdots + \bar{u}_\lambda\gamma^{(\lambda)}$ modulo p ganz ist, also ganze Koeffizienten $\bar{u}_i$ hat, so folgt aus der Gleichung:

$$u_1\gamma^{(1)} + \cdots + u_\lambda\gamma^{(\lambda)} = p^\delta(\bar{u}_1\gamma^{(1)} + \cdots + \bar{u}_\lambda\gamma^{(\lambda)}),$$

daß allgemein $\bar{u}_i = p^\delta\bar{u}_i$ sein muß, w. z. b. w. Dieser Beweis gilt auch für Potenzen p^δ von p mit negativen Exponenten.

Zwei Zahlen γ und γ' heißen **modulo p^δ kongruent**, wenn ihre Differenz $\gamma - \gamma'$ durch p^δ algebraisch teilbar ist.

Ist

(3) $$\gamma = u_1\gamma^{(1)} + \cdots + u_\lambda\gamma^{(\lambda)}, \quad \gamma' = u_1'\gamma^{(1)} + \cdots + u_\lambda'\gamma^{(\lambda)},$$

so ist also $\gamma - \gamma'$ nur dann durch p^δ teilbar, wenn das gleiche für alle Differenzen $u_i - u_i'$ gilt, wenn also die λ Kongruenzen

(3a) $$u_i \equiv u_i' \pmod{p^\delta}$$

erfüllt sind.

Eine ganze Zahl:

$$\varepsilon = e_1\gamma^{(1)} + e_2\gamma^{(2)} + \cdots + e_\lambda\gamma^{(\lambda)},$$

deren λ Koeffizienten modulo p reduzierte ganze Zahlen, also Zahlen der Reihe $0, 1, \ldots p - 1$ sind, soll eine **modulo p reduzierte ganze Zahl des Bereiches $K(\alpha)$** heißen. Zwei solche reduzierte Zahlen ε und

$$\varepsilon' = e_1'\gamma^{(1)} + e_2'\gamma^{(2)} + \cdots + e_\lambda'\gamma^{(\lambda)}$$

sind nur dann modulo p kongruent, wenn sie gleich sind, weil jede Kongruenz $e_i \equiv e_i' \pmod{p}$ nur erfüllt ist, wenn $e_i = e_i'$ ist. Da jede er Zahlen e_i unabhängig von den anderen die Werte $0, 1, \ldots p - 1$

annehmen kann, so gibt es genau p^λ verschiedene modulo p reduzierte ganze Zahlen.

Jede modulo p ganze algebraische Zahl ist einer und nur einer reduzierten Zahl modulo p kongruent.

Ist nämlich $\gamma = u_1\gamma^{(1)} + \cdots + u_\lambda\gamma^{(\lambda)}$, wo die u_i modulo p ganze rationale Zahlen sind, so besteht ja für jeden Koeffizienten u_i eine Gleichung:

$$u_i = e_i^{(0)} + pu_i', \qquad (i = 1, 2, \cdots \lambda)$$

wo $e_i^{(0)}$ eine der Zahlen $0, 1, \ldots p-1$, und u_i' modulo p ganz ist. Also ergibt sich durch Multiplikation dieser Gleichungen mit $\gamma^{(i)}$ und Addition aller λ Gleichungen:

$$u_1\gamma^{(1)} + \cdots + u_\lambda\gamma^{(\lambda)} = e_1^{(0)}\gamma^{(1)} + \cdots + e_\lambda^{(0)}\gamma^{(\lambda)} + p(u_1'\gamma^{(1)} + \cdots + u_\lambda'p)$$

oder

(4) $$\gamma = \varepsilon^{(0)} + p\gamma',$$

wo

$$\varepsilon^{(0)} = \sum_i e_i^{(0)}\gamma^{(i)}$$

eine eindeutig bestimmte reduzierte und γ' eine modulo p ganze Zahl ist.

Mit Hilfe dieses Resultates leite ich nun eine Darstellung der modulo p ganzen algebraischen Zahlen her, welche eine direkte Verallgemeinerung der in (2) a. S. 5 gegebenen Darstellung aller ganzen rationalen Zahlen im p-adischen Zahlensysteme ist.

Stellt man nämlich jetzt γ' in (4) in derselben Weise dar, wie vorher γ und fährt so fort, so erhält man eine Reihe von Gleichungen:

(4a) $$\begin{aligned} \gamma' &= \varepsilon^{(1)} + p\gamma'', \\ \gamma'' &= \varepsilon^{(2)} + p\gamma''', \\ &\vdots \\ \gamma^{(\nu)} &= \varepsilon^{(\nu)} + p\gamma^{(\nu+1)}. \end{aligned}$$

Multipliziert man nun die Gleichungen (4) und (4a) der Reihe nach mit $1, p, p^2 \ldots p^\nu$, addiert sie und läßt die sich auf beiden Seiten forthebenden Glieder fort, so ergibt sich für jedes beliebige ν eine Gleichung:

(5) $$\gamma = \varepsilon^{(0)} + p\varepsilon^{(1)} + p^2\varepsilon^{(2)} + \cdots + p^\nu\varepsilon^{(\nu)} + p^{\nu+1}\gamma^{(\nu+1)},$$

wo die Koeffizienten $\varepsilon^{(0)}, \varepsilon^{(1)} \ldots$ eindeutig bestimmte reduzierte Zahlen sind, und $\gamma^{(\nu+1)}$ eine modulo p ganze algebraische Zahl bedeutet.

Eine beliebige modulo p ganze algebraische Zahl γ ist also für jede noch so hohe Potenz $p^{\nu+1}$ von p einer Zahl

$$\varepsilon^{(0)} + \varepsilon^{(1)}p + \varepsilon^{(2)}p^2 + \cdots + \varepsilon^{(\nu)}p^\nu$$

kongruent, deren Koeffizienten $\varepsilon^{(i)}$ eindeutig bestimmte reduzierte Zahlen von $K(\alpha)$ sind.

Da jede gebrochene Zahl $\delta = \frac{\gamma}{p^\varrho}$ ist, wo γ algebraisch ganz ist, so erhält man für jede gebrochene Zahl ohne weiteres eine Gleichung:

$$(5a)\quad \delta = \frac{\varepsilon^{(-\varrho)}}{p^\varrho} + \frac{\varepsilon^{-(\varrho-1)}}{p^{\varrho-1}} + \cdots + \frac{\varepsilon^{(-1)}}{p} + \varepsilon^{(0)} + \cdots + \varepsilon^{(\nu)} p^\nu + \gamma^{(\nu+1)} p^{\nu+1}.$$

Also ergibt sich der folgende Satz:

Jede Zahl von $K(\alpha)$ ist für eine beliebig hohe Potenz $p^{\nu+1}$ von p als Modul einer Reihe

$$\varepsilon^{(r)} p^r + \varepsilon^{(r+1)} p^{r+1} + \cdots + \varepsilon^{(\nu)} p^\nu$$

kongruent, deren Koeffizienten eindeutig bestimmte reduzierte Zahlen von $K(\alpha)$ sind, und diese Reihe beginnt dann und nur dann mit einer endlichen Anzahl negativer Potenzen von p, wenn die zu untersuchende Zahl modulo p gebrochen ist.

Entwickelt man die λ rationalen Koeffizienten u_i einer Zahl von $K(\alpha)$:

$$(6)\qquad \gamma = u_1 \gamma^{(1)} + \cdots + u_\lambda \gamma^{(\lambda)},$$

nach Potenzen von p, so daß also:

$$(6a)\qquad u_i = e_i^{(r)} p^r + e_i^{(r+1)} p^{r+1} + \cdots \quad (p) \qquad (i = 1, 2, \cdots \lambda)$$

ist, und faßt dann die mit denselben Potenzen $p^r, p^{r+1} \ldots$ von p multiplizierten Glieder zusammen, so erhält man eine Reihe:

$$(7)\qquad \varepsilon^{(r)} p^r + \varepsilon^{(r+1)} p^{r+1} + \cdots + \varepsilon^{(\nu)} p^\nu + \cdots$$

mit eindeutig bestimmten modulo p reduzierten Koeffizienten, welche im allgemeinen ins Unendliche fortgeht, und man erkennt sofort, daß für jede Potenz $p^{\nu+1}$ von p

$$(7a)\qquad \gamma \equiv \varepsilon^{(r)} p^r + \varepsilon^{(r+1)} p^{r+1} + \cdots + \varepsilon^{(\nu)} p^\nu \pmod{p^{\nu+1}}$$

ist, wo auf der rechten Seite derjenige Teil unserer Reihe (7) steht, welchen man bei Fortlassung aller mit $p^{\nu+1}, p^{\nu+2}, \ldots$ multiplizierten Glieder erhält.

Da die Koeffizienten u_i von γ rationale Zahlen sind, so ergeben ihre Entwicklungen (6a), lauter rein oder gemischt periodische p-adische Reihen. Hieraus folgt leicht, daß auch die modulo p reduzierten algebraischen Zahlen $\varepsilon^{(r)}, \varepsilon^{(r+1)}, \ldots$ eine reine oder gemischt periodische Reihe ergeben. Jede algebraische Zahl γ von $K(\alpha)$ steht also zu einer einzigen solchen periodischen Reihe in der durch die Kongruenzen (7a) angegebenen Beziehung, und umgekehrt würde man sich sehr leicht überzeugen, daß durch jede periodische Reihe

$$\varepsilon^{(r)} p^r + \varepsilon^{(r+1)} p^{r+1} + \cdots$$

eine algebraische Zahl des Bereiches $K(\alpha)$ eindeutig bestimmt wird, für welche die Kongruenzen (7a) in bezug auf jede noch so hohe Potenz $p^{\nu+1}$ von p als Modul erfüllt sind.

Von dieser Tatsache ausgehend, erweiterten wir im zweiten Kapitel den Bereich $K(1)$ der rationalen Zahlen in der Weise, daß wir die Gesamtheit aller Reihen:

$$e^{(r)}p^r + e^{(r+1)}p^{r+1} + \cdots$$

mit modulo p reduzierten ganzen rationalen Koeffizienten $e^{(i)}$ als sog. p-adische Zahlen, d. h. Zahlgrößen eines größeren Bereiches $K(p)$ definierten, für diese den Begriff der Gleichheit zweier Zahlgrößen definierten und auf Grund dieser Definition die elementaren Rechenoperationen einwandsfrei und so definierten, daß sie für den engeren Bereich $K(1)$ der rationalen Zahlen gültig bleiben.

Genau in derselben Weise will ich nun den Bereich $K(\alpha)$ der rationalen Funktionen von α erweitern: Es sei α wie vorher eine algebraische Zahl λ^{ter} Ordnung, $K(\alpha)$ der durch α konstituierte Körper, $(\gamma^{(1)}, \gamma^{(2)}, \ldots \gamma^{(\lambda)})$ ein ein- für allemal fest gewähltes Fundamentalsystem modulo p; es werde durch

$$\varepsilon = e_1\gamma^{(1)} + e_2\gamma^{(2)} + \cdots + e_\lambda\gamma^{(\lambda)} \qquad (e_i = 0, 1, \cdots p-1)$$

allgemein jede modulo p reduzierte algebraische Zahl bezeichnet. Ich betrachte dann den Bereich aller Zahlgrößen:

$$(8) \qquad \gamma = \varepsilon^{(r)}p^r + \varepsilon^{(r+1)}p^{r+1} + \cdots,$$

deren Koeffizienten $\varepsilon^{(i)}$ modulo p reduzierte Zahlen von $K(\alpha)$ sind, welche nach einem gegebenen Bildungsgesetze beliebig weit berechnet werden können. Die Gesamtheit aller dieser Zahlgrößen nenne ich die p-adischen algebraischen Zahlen des Körpers $K(\alpha)$ oder kürzer die Zahlen des Körpers $K(p, \alpha)$. Diese algebraischen p-adischen Zahlen unterscheiden sich von den im zweiten Kapitel allein betrachteten rationalen p-adischen Zahlen

$$e^{(r)}p^r + e^{(r+1)}p^{r+1} + \cdots \qquad (e^{(k)} = 0, 1, \cdots p-1)$$

allein dadurch, daß bei jenen die Koeffizienten $e^{(k)}$ wohl definierte modulo p reduzierte ganze rationale Zahlen waren, während die jetzt auftretenden Koeffizienten $\varepsilon^{(k)}$ wohl definierte modulo p reduzierte ganze algebraische Zahlen des Körpers $K(\alpha)$ sind. Es wird sich aber zeigen, daß alle für die rationalen p-adischen Zahlen geltenden Rechnungsgesetze für die algebraischen p-adischen Zahlen unverändert gültig bleiben.

Eine p-adische algebraische Zahl γ heißt gebrochen oder ganz, je nachdem ihre Entwicklung (8) mit einer negativen Potenz von p beginnt oder nicht. Der Einfachheit wegen betrachte ich im folgenden zunächst nur ganze Zahlen

$$\gamma = \varepsilon^{(0)} + \varepsilon^{(1)}p + \varepsilon^{(2)}p^2 + \cdots + \varepsilon^{(k)}p^k + \cdots \quad (p),$$

von deren Anfangskoeffizienten $\varepsilon^{(0)}, \varepsilon^{(1)}, \ldots$ auch gewisse Null sein können; ich bemerke aber, daß alle Definitionen und Sätze wörtlich ebenso für modulo p gebrochene Zahlen gelten. Ich schreibe diese Zahlgrößen abgekürzt in der Form:

(8a) $$\gamma = \varepsilon^{(0)}, \varepsilon^{(1)}\varepsilon^{(2)}\ldots$$

und nenne wieder die reduzierten algebraischen Zahlen $\varepsilon^{(0)}, \varepsilon^{(1)}, \ldots$ die Ziffern der Zahl γ. Die gebrochenen Zahlen:

(8b) $$\delta = \varepsilon^{(-\varrho)}\ldots\varepsilon^{(-1)}\varepsilon^{(0)}, \varepsilon^{(1)}\varepsilon^{(2)}\ldots,$$

unterscheiden sich nur dadurch von den ganzen p-adischen Zahlen, daß vor dem Komma noch mehr als eine Ziffer steht.

Ich nenne die gewöhnliche algebraische Zahl des Bereiches $K(\alpha)$:

$$\gamma^{(k)} = \varepsilon^{(0)} + \varepsilon^{(1)}p + \cdots + \varepsilon^{(k)}p^k = \varepsilon^{(0)}, \varepsilon^{(1)}\ldots\varepsilon^{(k)},$$

welche aus der p-adischen Zahl γ entsteht, wenn man alle durch p^{k+1} teilbaren Glieder fortläßt, den k^{ten} Näherungswert von γ. Diese Näherungswerte:

(9) $$\gamma^{(0)} = \varepsilon^{(0)}, \quad \gamma^{(1)} = \varepsilon^{(0)}, \varepsilon^{(1)}, \quad \gamma^{(2)} = \varepsilon^{(0)}, \varepsilon^{(1)}\varepsilon^{(2)}, \ldots$$

bilden dann eine eindeutig bestimmte Reihe von wohldefinierten ganzen algebraischen Zahlen des Bereiches $K(\alpha)$, für welche allgemein

$$\gamma^{(k)} = \gamma^{(k-1)} + \varepsilon^{(k)}p^k$$

oder

(9a) $$\gamma^{(k)} \equiv \gamma^{(k-1)} \pmod{p^k}$$

ist. Ist $\delta = \varepsilon^{(-r)}\ldots\varepsilon^{(0)}, \varepsilon^{(1)}\varepsilon^{(2)}\ldots$ eine gebrochene Zahl, so besitzt sie auch von Null verschiedene Näherungswerte negativer Ordnung:

(9b) $$\delta^{(-r)} = \frac{\varepsilon^{(-r)}}{p^r}, \qquad \delta^{-(r-1)} = \frac{\varepsilon^{-(r)}}{p^r} + \frac{\varepsilon^{-(r-1)}}{p^{r-1}}, \ldots,$$

und man erkennt sofort die Richtigkeit des Satzes:

> Eine p-adische algebraische Zahl ist gebrochen oder ganz, je nachdem alle ihre Näherungswerte gebrochene oder ganze Zahlen des Bereiches $K(\alpha)$ sind.
>
> Zwei Zahlen des Bereiches $K(p, \alpha)$
>
> $$\gamma = \varepsilon^{(0)}, \varepsilon^{(1)}\ldots\varepsilon^{(k)}\varepsilon^{(k+1)}\ldots; \quad \gamma' = \varepsilon^{(0)}, \varepsilon^{(1)}\ldots\varepsilon^{(k)}\bar{\varepsilon}^{(k+1)}\ldots$$
>
> heißen kongruent modulo p^{k+1}, wenn ihre k^{ten} Näherungswerte $\gamma^{(k)}$ und $\gamma'^{(k)}$ noch gleich sind, während $\gamma^{(k+1)}$ und $\gamma'^{(k+1)}$ schon verschieden sein können. Dies ist dann und nur dann der Fall, wenn die Ziffern $\varepsilon^{(0)}, \varepsilon^{(1)}, \ldots$ bis $\varepsilon^{(k)}$ in beiden Zahlen dieselben sind.

Zwei Zahlen γ und γ' des Bereiches $K(p, \alpha)$ sollen **gleich für den Bereich von p** heißen, wenn ihre Näherungswerte

$$\gamma^{(0)}, \gamma^{(1)}, \gamma^{(2)}, \ldots; \quad \gamma'^{(0)}, \gamma'^{(1)}, \gamma'^{(2)}, \ldots$$

von genügend hoher Ordnung für jede noch so hohe Potenz von p als Modul kongruent sind, und dies ist wieder offenbar nur dann der Fall, wenn ihre Entwicklungskoeffizienten $\varepsilon^{(r)}$ und $\varepsilon'^{(r)}$ für jeden Index r gleich sind. Eine Zahl γ ist speziell gleich Null, wenn ihre Näherungswerte $\gamma^{(r)}$ durch jede noch so hohe Potenz von p teilbar sind, falls man nur den Index r groß genug wählt.

Bei dieser Definition der Gleichheit kann eine Zahl $\gamma = \varepsilon^{(0)}, \varepsilon^{(1)} \varepsilon^{(2)} \ldots$ mit den Näherungswerten $\gamma^{(0)}, \gamma^{(1)}, \ldots$ auch als der Grenzwert ihrer Näherungswerte, d. h. durch die Gleichung:

$$\gamma = \lim_{k=\infty} \gamma^{(k)} \qquad (p)$$

definiert werden.

Wir werden mitunter von der Beschränkung absehen, daß die Ziffern $\varepsilon^{(i)}$ modulo p **reduzierte** ganze Zahlen sind, und auch Zahlen

$$\gamma = \bar{\varepsilon}^{(0)} + \bar{\varepsilon}^{(1)} p + \cdots$$

in den Kreis unserer Betrachtung ziehen, deren Koeffizienten beliebige, aber wohldefinierte modulo p ganze Zahlen des Bereiches $K(\alpha)$ sind. Durch die a. S. 21 flgde. angewandten Methoden beweist man dann auch hier die Richtigkeit des Satzes:

Jede nicht reduzierte Zahl ist einer eindeutig bestimmten reduzierten Zahl für den Bereich von p gleich.

Ebenso wie innerhalb des Bereiches $K(p)$ definieren wir auch hier die Summe, die Differenz und das Produkt zweier p-adischen algebraischen Zahlen

$$\gamma = \varepsilon^{(0)}, \varepsilon^{(1)} \varepsilon^{(2)} \ldots \quad \delta = \delta^{(0)}, \delta^{(1)} \delta^{(2)} \ldots \qquad (p)$$

durch die Gleichungen:

$$\text{(10)} \qquad \begin{aligned} \gamma \pm \delta &= \lim_{k=\infty} (\gamma^{(k)} \pm \delta^{(k)}) \\ \gamma\delta &= \lim_{k=\infty} (\gamma^{(k)} \delta^{(k)}) \end{aligned} \qquad (p),$$

und wir beweisen, wie a. a. O. a. S. 24 flgde., daß jede dieser drei elementaren Operationen zu einer eindeutig bestimmten p-adischen Zahl hinführt.

In der Tat ergibt sich aus diesen Definitionen, daß sich die Summe, die Differenz und das Produkt zweier Zahlen des Bereiches $K(p, \alpha)$

$$\gamma = \varepsilon^{(0)} + \varepsilon^{(1)} p + \varepsilon^{(2)} p^2 + \cdots; \quad \delta = \delta^{(0)} + \delta^{(1)} p + \cdots \qquad (p)$$

in ihrer nicht reduzierten Form folgendermaßen darstellt:

$$\gamma \pm \delta = (\varepsilon^{(0)} \pm \xi^{(0)}) + p(\varepsilon^{(1)} \pm \xi^{(1)}) + \cdots$$
$$\gamma\delta = \varepsilon^{(0)}\xi^{(0)} + p(\varepsilon^{(0)}\xi^{(1)} + \varepsilon^{(1)}\xi^{(0)}) + \cdots,$$

aus denen sich ihre reduzierte Form eindeutig bestimmt.

§ 3. Der Körper $K(p, \alpha)$, dessen Grundgleichung für den Bereich von p unzerlegbar ist.

Für die eingehendere Untersuchung der p-adischen algebraischen Zahlen, zu der ich jetzt übergehe, ist die folgende andere Darstellung derselben von besonderer Wichtigkeit: Im vorigen Paragraphen zeigte ich, daß alle p-adischen algebraischen Zahlen in der Form:

$$(1) \qquad \gamma = u_1\gamma^{(1)} + u_2\gamma^{(2)} + \cdots + u_\lambda\gamma^{(\lambda)} \quad (p)$$

darstellbar sind, wo $(\gamma^{(1)}, \ldots \gamma^{(\lambda)})$ die Elemente eines Fundamentalsystems für den Körper $K(\alpha)$, und die Koeffizienten u_i beliebige rationale p-adische Zahlen sind. Da nun jede der λ algebraischen Zahlen $\gamma^{(i)}$ eine rationale Funktion von α mit gewöhnlichen rationalen Koeffizienten ist, so sieht man, daß jede p-adische Zahl des Bereiches in der Form:

$$(2) \qquad \gamma = \varphi(\alpha)$$

darstellbar ist, wo $\varphi(\alpha)$ eine rationale Funktion von α mit rationalen p-adischen Koeffizienten bedeutet. Aber auch umgekehrt ist jede solche rationale Funktion, deren Nenner von Null verschieden ist, wie ich a. S. 133 zeigen werde, gleich einer p-adischen Zahl (1). Da somit die Untersuchung der Zahlen (2) mit derjenigen der p-adischen algebraischen Zahlen (1) völlig zusammenfällt, so will ich bei den weiteren Betrachtungen von der Darstellung (2) der Zahlen des Bereiches $K(p, \alpha)$ ausgehen.

Diese Untersuchung der p-adischen algebraischen Zahlen (2) des Bereiches $K(p, \alpha)$, d. h. der rationalen Funktionen von α mit p-adischen Koeffizienten führt nun im wesentlichen zu denselben Resultaten, wie die im fünften Kapitel durchgeführte Untersuchung der algebraischen Zahlen des Körpers $K(\alpha)$, d. h. der rationalen Funktionen von α mit gewöhnlichen rationalen Koeffizienten. Der einzige, aber allerdings sehr wichtige Unterschied besteht darin, daß wir a. a. O. von vornherein die Grundgleichung für α:

$$(3) \qquad f(x) = x^\lambda + a_1x^{\lambda-1} + \cdots + a_\lambda = 0$$

im Bereiche $K(1)$ der rationalen Zahlen irreduktibel annahmen; denn hieraus folgt ja im allgemeinen noch keineswegs, daß diese Gleichung auch für den größeren Bereich $K(p)$ der p-adischen Zahlen ebenfalls

unzerlegbar sein muß. Auch dieser Unterschied fällt aber fort, wenn wir voraussetzen können, daß $f(x)$ nicht bloß innerhalb des Körpers $K(1)$, sondern auch innerhalb des Körpers $K(p)$ nicht in Faktoren niedrigeren Grades zerlegt werden kann.

Wir können und wollen für die weitere Untersuchung diese Annahme machen, denn einmal sind wir nach den Ergebnissen des vierten Kapitels imstande, zu entscheiden, ob eine vorgelegte Funktion $f(x)$ innerhalb $K(p)$ irreduktibel ist oder nicht, und zweitens wird sich zeigen, daß alle später zur Untersuchung gelangenden Grundgleichungen (3) wirklich auch für den Bereich von p unzerlegbar sind.

Es sei also jetzt die Grundgleichung (3) auch für den Bereich von p irreduktibel; $\alpha_1, \alpha_2, \ldots \alpha_\lambda$ seien wieder ihre Wurzeln, und α bezeichne irgend eine unter ihnen. Der Grund, warum nun alle Sätze über die Zahlen des Körpers $K(p, \alpha)$ mit den entsprechenden für den Körper $K(\alpha)$ übereinstimmen, ist der, daß unter der soeben gemachten Voraussetzung auch für den Bereich $K(p, \alpha)$ der Fundamentalsatz besteht:

> Eine Wurzel α der irreduktiblen Gleichung (3) genügt dann und nur dann für den Bereich von p einer anderen Gleichung:
>
> (4) $$g(x) = g_0 x^m + g_1 x^{m-1} + \cdots + g_m = 0 \qquad (p),$$
>
> deren Koeffizienten rationale p-adische Zahlen sind, wenn ihre linke Seite für den Bereich von p durch $f(x)$ teilbar, wenn also
>
> $$g(x) = f(x)\, h(x) \qquad (p)$$
>
> ist.

Hier werde aber noch einmal darauf aufmerksam gemacht, daß die Aussage, α sei für den Bereich von p eine Wurzel der Gleichung (4) mit p-adischen Koeffizienten, etwas völlig anderes bedeutet als die, daß α der Größe nach einer Gleichung mit rationalen Koeffizienten genügt; nach der a. S. 128 oben angegebenen Definition ist nämlich

$$g(\alpha) = 0, \qquad (p)$$

wenn die Näherungswerte genügend hoher Ordnung von $g(\alpha)$ durch jede noch so hohe Potenz von p algebraisch teilbar sind.

Der Beweis dieses Satzes ist sehr einfach; angenommen $g(x)$ wäre durch $f(x)$ nicht teilbar, so sind die beiden Funktionen $f(x)$ und $g(x)$ wegen der Irreduktibilität von $f(x)$ teilerfremd; man kann also durch das Euklidische Verfahren zwei Multiplikatoren $f_1(x)$ und $g_1(x)$ so bestimmen, daß

$$f(x) f_1(x) + g(x) g_1(x) = 1 \quad (p)$$

ist. Setzt man aber in dieser Gleichung $x = \alpha$, so würde sich $0 = 1$ ergeben; da unsere letzte Annahme somit auf einen Widerspruch führt, so ist der Satz bewiesen. Hieraus folgen sofort die beiden Sätze:

Eine Gleichung:

(5) $$g(\alpha_1) = 0 \quad (p)$$

mit rationalen p-adischen Koeffizienten bleibt richtig, wenn man α_1 der Reihe nach durch die konjugierten Zahlen $\alpha_2, \dots \alpha_\lambda$ ersetzt.

Eine Gleichung von niedrigerem als dem λ^{ten} Grade:

$$g(x) = g_1 x^{\lambda-1} + \cdots + g_\lambda = 0 \quad (p)$$

mit p-adischen Koeffizienten kann nur dann die Wurzel $x = \alpha$ haben, wenn alle Koeffizienten g_i für den Bereich von p gleich Null sind.

Ich betrachte nun die Gesamtheit aller rationalen Funktionen von α

(6) $$\beta = \varphi(\alpha) \quad (p)$$

mit beliebigen p-adischen Koeffizienten und zeige, daß für sie wörtlich dieselben Gesetze bestehen wie für den Körper $K(\alpha)$ der rationalen Funktionen von α mit gewöhnlichen rationalen Koeffizienten.

Zu jeder Zahl $\beta_1 = \varphi(\alpha_1)$ gehören die λ konjugierten Zahlen $\beta_1, \beta_2, \dots \beta_\lambda$, wo allgemein:

(6a) $$\beta_i = \varphi(\alpha_i) \quad (p)$$

ist, und diese genügen der Gleichung λ^{ten} Grades:

(6b) $$g(y) = (y - \beta_1)(y - \beta_2) \cdots (y - \beta_\lambda) = y^\lambda + b_1 y^{\lambda-1} + \cdots + b_\lambda = 0 \quad (p),$$

deren Koeffizienten als symmetrische Funktionen von $(\alpha_1, \alpha_2, \dots \alpha_\lambda)$ mit rationalen p-adischen Koeffizienten offenbar ebenfalls rationale p-adische Zahlen sind (vgl. S. 98 oben).

Die linke Seite $g(y)$ dieser Gleichung ist für den Bereich der rationalen p-adischen Zahlen entweder selbst irreduktibel oder sie ist eine Potenz einer irreduktiblen Funktion desselben Bereiches. Zerfällt nämlich $g(y)$ in mehrere Faktoren, wovon man sich nach dem soeben erwähnten Satze a. S. 68 oben durch eine endliche Anzahl von Versuchen überzeugen kann, und ist $g_1(y)$ etwa derjenige unter den irreduktiblen Faktoren, welcher für $y = \beta_1 = \varphi(\alpha_1)$ für den Bereich von p gleich Null wird, so folgt aus dem soeben bewiesenen Satze (5), daß die Gleichung $g_1(\beta_1) = g_1(\varphi(\alpha_1)) = 0$ richtig bleibt, wenn man in ihr α_1 durch $\alpha_2, \dots \alpha_\lambda$ ersetzt; die irreduktible Funktion $g_1(y)$ besitzt also jede der Wurzeln $\beta_1, \beta_2, \dots \beta_\lambda$, und da dasselbe für alle irreduktiblen Faktoren gilt, so sind diese sämtlich gleich, d. h. es ist

(6c) $$g(y) = (g_1(y))^\nu \quad (p),$$

wo $g_1(y)$ eine für den Bereich von p irreduktible Funktion des μ^{ten} Grades und $\mu\nu = \lambda$ ist.

Eine p-adische Zahlgröße $\beta = \varphi(\alpha)$ heißt wieder **algebraisch ganz**, wenn die Koeffizienten der Gleichung $g(y) = 0$ oder, was dasselbe ist, die Koeffizienten der irreduktiblen Gleichung $g_1(y) = 0$ in (6c), der β nebst ihren konjugierten genügt, ganze p-adische Zahlen sind. Ist speziell β eine modulo p ganze Zahl des Bereiches $K(\alpha)$, (vgl. S. 119 (III)), so ist sie offenbar auch nach der hier aufgestellten Definition algebraisch ganz. Endlich ergibt sich durch die a. S. 99 ausgeführten Betrachtungen, daß die Summe, die Differenz und das Produkt von algebraisch ganzen Zahlen wieder algebraisch ganz ist.

Man kann auch hier alle ganzen algebraischen Zahlgrößen durch ein Fundamentalsystem darstellen. Ist nämlich wieder

(7) $$\gamma^{(1)}, \gamma^{(2)}, \dots \gamma^{(\lambda)}$$

ein Fundamentalsystem modulo p für die ganzen algebraischen Zahlen des Bereiches $K(\alpha)$, so sind diese ja auch nach der soeben gegebenen Definition algebraisch ganz, und daher ist auch jede Zahl

$$u_1 \gamma^{(1)} + \cdots + u_\lambda \gamma^{(\lambda)}$$

algebraisch ganz, wenn ihre Koeffizienten u_i ganze rationale p-adische Zahlen sind. Andererseits zeigt man genau ebenso, wie a. S. 121 Mitte, daß eine Zahlgröße:

$$\frac{v_1 \gamma^{(1)} + \cdots + v_\lambda \gamma^{(\lambda)}}{p}$$

mit ganzen p-adischen Koeffizienten v_i nur dann algebraisch ganz sein kann, wenn alle Koeffizienten v_i durch p teilbar sind, und damit ist unsere Behauptung bewiesen.

Ebenso beweist man genau, wie a. S. 122 unten, daß ein System $(\delta^{(1)}, \delta^{(2)}, \dots \delta^{(\lambda)})$ von λ ganzen p-adischen Zahlen des Bereiches $K(p, \alpha)$ dann und nur dann ein Fundamentalsystem ist, wenn die Determinante $|c_{ik}|$ der ganzzahligen Substitution

$$\delta^{(i)} = \sum_k c_{ik} \gamma^{(k)} \quad (p) \qquad (i = 1, 2, \cdots \lambda)$$

durch welche das System $(\delta^{(i)})$ mit dem Fundamentalsystem $(\gamma^{(i)})$ zusammenhängt, eine Einheit für den Bereich von p ist.

Es sei nun $\beta = \varphi(\alpha)$ irgend eine rationale Funktion von α mit Koeffizienten des Bereiches $K(p)$. Ist dann $(\gamma^{(1)}, \gamma^{(2)}, \dots \gamma^{(\lambda)})$ das oben in (7) eingeführte Fundamentalsystem, so ist nach dem soeben geführten Beweise die Größe β durch dieses in der Form:

$$\beta = u_1 \gamma^{(1)} + \cdots + u_\lambda \gamma^{(\lambda)}$$

darstellbar, wo die Koeffizienten

$$u_i = e_i^{(r)} p^r + e_i^{(r+1)} p^{r+1} + \cdots \qquad (i = 1, 2, \cdots \lambda)$$

ganze oder gebrochene Zahlen von $K(p)$ sind, und r die niedrigste Ordnungszahl der λ Koeffizienten u_i ist. Setzt man diese Werte ein und faßt die mit $p^r, p^{r+1}, \ldots$ multiplizierten Glieder zusammen, so ergibt sich für β die Darstellung:

(8) $$\beta = \varepsilon^{(r)} p^r + \varepsilon^{(r+1)} p^{r+1} + \cdots \quad (p),$$

wo die Koeffizienten $\varepsilon^{(r)}, \varepsilon^{(r+1)} \ldots$ eindeutig bestimmte modulo p reduzierte Zahlen sind. Jede rationale Funktion $\beta = \varphi(\alpha)$ läßt sich also nach Potenzen von p so entwickeln, daß die Koeffizienten modulo p reduzierte Zahlen von $K(\alpha)$ sind. Jede solche rationale Funktion von α mit p-adischen Koeffizienten ist also einer eindeutig bestimmten p-adischen algebraischen Zahl $\sum \varepsilon^{(i)} p^i$ gleich.

Umgekehrt ist aber, wie a. S. 129 bei (1) bewiesen wurde, jede p-adische algebraische Zahl $\sum \varepsilon^{(i)} p^i$ des Bereiches $K(p, \alpha)$ einer rationalen Funktion $\varphi(\alpha)$ von α mit rationalen p-adischen Koeffizienten gleich. Also ergibt sich der bereits a. S. 129 angekündigte Satz:

> Der Körper $K(p, \alpha)$ aller p-adischen algebraischen Zahlen $\sum \varepsilon^{(k)} p^k$ ist mit der Gesamtheit $\beta = \varphi(\alpha)$ aller rationalen Funktionen von α mit rationalen p-adischen Koeffizienten identisch.

Der Bereich $K(\alpha)$ aller rationalen Funktionen von α mit rationalen Zahlkoeffizienten des Bereiches $K(1)$ bildet einen Teilbereich von $K(p, \alpha)$, nämlich denjenigen, bei welchem alle Zahlkoeffizienten periodisch sind.

Beachtet man ferner, daß die Gleichung (8) für β richtig bleibt, wenn man in ihr α der Reihe nach durch $\alpha_1, \alpha_2, \ldots \alpha_\lambda$ ersetzt, und daß bei diesen Substitutionen β und die $\varepsilon^{(k)}$ bzw. durch die konjugierten Zahlen $\beta_1, \ldots \beta_\lambda$ und $\varepsilon_1^{(k)}, \ldots \varepsilon_\lambda^{(k)}$ ersetzt werden, so ergibt sich schließlich das Resultat:

> Ist $\beta = \varphi(\alpha)$ irgend eine rationale Funktion von α, deren Koeffizienten rationale p-adische Zahlen sind, so lassen sich die λ konjugierten Zahlen β_i in einen Zyklus konjugierter Reihen:
>
> (9) $$\beta_i = \varepsilon_i^{(r)} p^r + \varepsilon_i^{(r+1)} p^{r+1} + \cdots \qquad (i = 1, 2, \cdots \lambda)$$
>
> entwickeln, welche nach ganzen Potenzen von p fortschreiten und deren Koeffizienten eindeutig bestimmte modulo p reduzierte Zahlen von $K(\alpha)$ sind.

§ 4. Die Einheiten des algebraischen Körpers $K(p, \alpha)$.

Die Untersuchung der p-adischen algebraischen Zahlen $\beta = \varphi(\alpha)$ des Körpers $K(p, \alpha)$ in bezug auf die Primzahl p gestaltet sich nun wunderbar einfach:

Jede Zahl β genügt nebst ihren λ konjugierten einer Gleichung λ^{ten} Grades, welche ich jetzt in ihrer primitiven Form schreibe:

(1) $$G(y) = B_0 y^\lambda + B_1 y^{\lambda-1} + \cdots + B_\lambda = 0 \qquad (p);$$

ihre Koeffizienten B_i sind also ganze Zahlen von $K(p)$, welche nicht alle durch p teilbar sind. Die Funktion $G(y)$ ist entweder irreduktibel oder die Potenz einer irreduktiblen Funktion. Die reziproke Zahl $\beta' = \frac{1}{\beta}$ genügt der Gleichung:

(1a) $$G'(z) = B_\lambda z^\lambda + B_{\lambda-1} z^{\lambda-1} + \cdots + B_0 = 0 \qquad (p),$$

in welcher die Reihenfolge der Koeffizienten die entgegengesetzte ist.

Die Zahl β ist nun dann und nur dann algebraisch ganz, wenn der Koeffizient B_0 eine Einheit ist, denn nur dann besitzt die Gleichung für β:

(1b) $$y^\lambda + \frac{B_1}{B_0} y^{\lambda-1} + \cdots + \frac{B_\lambda}{B_0} = 0$$

lauter modulo p ganze Koffizienten; die Zahl $\frac{1}{\beta}$ ist algebraisch ganz oder gebrochen, je nachdem B_λ eine Einheit ist oder nicht.

Nach dem a. S. 74 Mitte bewiesenen Satze kann aber $G(y)$ nur dann selbst irreduktibel oder die Potenz einer irreduktiblen Funktion sein, wenn von den beiden äußeren Koeffizienten B_0 und B_λ mindestens einer eine Einheit modulo p ist. Hieraus in Verbindung mit den soeben gemachten Bemerkungen folgt also der einfache und höchst wichtige Satz:

I) Von zwei beliebigen reziproken algebraischen Zahlen β und $\frac{1}{\beta}$ ist stets mindestens eine für den Bereich von p algebraisch ganz.

Dieser Satz gilt auch für jede rationale p-adische Zahl, denn von zwei reziproken rationalen Zahlen:

(2) $$B = p^b \cdot E, \quad \frac{1}{B} = p^{-b} \cdot \frac{1}{E} = p^{-b} \cdot \overline{E}$$

ist ja diejenige ganz, für welche der Exponent von p nicht negativ ist. Im Bereiche der gewöhnlichen Zahlen gilt dagegen dieser Satz nicht mehr, falls wir eine Zahl durch eine andere teilbar nennen, wenn der Quotient eine ganze rationale Zahl ist. So sind in diesem Sinne die beiden reziproken Zahlen $\frac{4}{9}$ und $\frac{9}{4}$ gebrochen. Dagegen ist für den Bereich der Primzahl 3 die erste gebrochen und die zweite ganz, für den Bereich von 2 die erste ganz und die zweite gebrochen.

Nur aus dem Grunde gilt auch für den hier betrachteten Bereich $K(p, \alpha)$ derselbe einfache Satz wie für den Bereich $K(p)$, weil wir

die Grundgleichung für α auch für den Bereich von p als irreduktibel annehmen konnten.

Genügt die Zahl β der Gleichung (1), so ist

$$n(\beta) = \beta_1\beta_2\cdots\beta_\lambda = (-1)^\lambda\cdot\frac{B_\lambda}{B_0}, \tag{2a}$$

und diese Zahl ist ganz oder gebrochen, jenachdem B_λ eine Einheit oder durch p teilbar ist, jenachdem also β algebraisch ganz ist oder nicht. Wir können daher den folgenden einfachen Satz aussprechen:

II) Eine algebraische p-adische Zahl β des Bereiches $K(p, \alpha)$ ist dann und nur dann ganz, wenn ihre Norm $n(\beta)$ eine ganze p-adische Zahl ist*).

Mit Hilfe dieser Sätze können wir nun die algebraischen genau ebenso wie die rationalen p-adischen Zahlen in zwei Klassen einteilen, nämlich in Einheiten und Nichteinheiten.

III) Eine p-adische algebraische Zahl ε heißt eine Einheit, wenn sowohl sie, als ihr reziproker Wert $\frac{1}{\varepsilon}$ ganz ist.

Dieselbe Definition gilt auch für den Bereich der rationalen p-adischen Zahlen; denn die Zahlen B und $\frac{1}{B}$ in (2) sind dann und nur dann beide ganz, wenn $b = 0$, also $B = E$ ist.

Nach den soeben bewiesenen Sätzen II) und III) ist ε dann und nur dann eine algebraische Einheit, wenn

$$n(\varepsilon) \quad \text{und} \quad n\left(\frac{1}{\varepsilon}\right) = \frac{1}{n(\varepsilon)}$$

beide ganze p-adische Zahlen sind, und dies ist stets und nur dann der Fall, wenn $n(\varepsilon) = e_0 + e_1p + \cdots$ eine Einheit ist.

IV) Alle und nur die Zahlen ε sind also algebraische Einheiten, deren Normen rationale Einheiten sind.

Sind ε und ε' zwei algebraische Einheiten, sind also $n(\varepsilon) = E$ und $n(\varepsilon') = E'$ rationale Einheiten, so sind

$$n(\varepsilon\varepsilon') = n(\varepsilon)\,n(\varepsilon') = EE',$$
$$n\left(\frac{\varepsilon}{\varepsilon'}\right) = \frac{n(\varepsilon)}{n(\varepsilon')} = \frac{E}{E'}$$

wieder Einheiten, und es gilt somit der Satz:

V) Das Produkt beliebig vieler Einheiten ist wieder eine Einheit, der Quotient zweier Einheiten ist wieder eine solche. Speziell folgt hieraus, daß jede positive oder negative Potenz einer Einheit wieder eine Einheit ist.

Ist irgend eine Potenz ε^ν einer algebraischen Zahl ε eine Einheit, so ist ε selbst eine Einheit; denn ist

*) Die Gleichung (1b) für β hat also stets und nur dann lauter ganzzahlige Koeffizienten, wenn ihr konstantes Glied $n(\beta)$ ganz ist.

$$n(\varepsilon^\nu) = (n(\varepsilon))^\nu$$

eine Einheit von $K(p)$, so kann ja $n(\varepsilon)$ auch nur eine Einheit desselben Bereiches sein.

Von zwei p-adischen algebraischen Zahlen α und β heißt **die erste durch die zweite teilbar**, wenn der Quotient $\gamma = \frac{\alpha}{\beta}$ algebraisch ganz ist*). Da, wie wir oben zeigten, von den beiden Zahlen

$$\gamma = \frac{\alpha}{\beta} \text{ und } \frac{1}{\gamma} = \frac{\beta}{\alpha}$$

mindestens eine algebraisch ganz ist, so ergibt sich der Satz:

VI) Von zwei p-adischen Zahlen α und β ist mindestens eine durch die andere teilbar.

Ist α durch β teilbar, also $\gamma = \frac{\alpha}{\beta}$ algebraisch ganz, so muß

$$n(\gamma) = \frac{n(\alpha)}{n(\beta)}$$

eine **ganze** rationale Zahl sein; es muß also $n(\alpha)$ von höherer oder mindestens von der gleichen Ordnung in bezug auf p sein, wie $n(\beta)$. Dann und nur dann ist auch $\frac{\beta}{\alpha} = \frac{1}{\gamma}$ eine ganze Zahl, also nicht bloß α durch β, sondern auch β durch α teilbar, wenn auch $\frac{n(\beta)}{n(\alpha)}$ ganz ist, wenn also $n(\beta)$ und $n(\alpha)$ dieselbe Ordnungszahl haben. Nur in diesem Falle ist $\frac{\alpha}{\beta} = \varepsilon$ eine Einheit, d. h. $\alpha = \beta\varepsilon$.

VII) Zwei p-adische Zahlen, welche sich nur um eine Einheit unterscheiden, von denen also jede durch die andere teilbar ist, sollen **äquivalente Zahlen** genannt werden.

Dann gilt also der Satz:

VIII) Von zwei Zahlen α und β ist stets diejenige durch die andere teilbar, deren Norm von höherer Ordnung ist; sie sind dann und nur dann äquivalent, wenn ihre Normen von gleicher Ordnung sind.

Zwei Zahlen α und α' des Körpers $K(p, \alpha)$ heißen **kongruent** modulo einer dritten Zahl β, wenn $\alpha - \alpha'$ durch β teilbar, wenn also $n(\alpha - \alpha')$ durch $n(\beta)$ teilbar ist. Schreiben wir jene Kongruenz wieder in der Form:

(3) $$\alpha \equiv \alpha' \pmod{\beta},$$

so kann diese auch durch die Kongruenz:

(3a) $$n(\alpha - \alpha') \equiv 0 \pmod{n(\beta)}$$

vollständig ersetzt werden. Da $n(\beta\varepsilon) = n(\beta)E$ dieselbe Ordnungszahl hat wie $n(\beta)$, so ergibt sich:

---

*) Wir drücken diese Tatsache wieder folgendermaßen aus:

$$\alpha \equiv 0 \pmod{\beta}.$$

IX) Eine jede Kongruenz (3) bleibt richtig, wenn man den Modul β durch irgend eine äquivalente Zahl $\beta\varepsilon$ ersetzt. Natürlich bleibt sie a fortiori richtig, wenn β durch irgend einen Teiler von β ersetzt wird.

Meistens werden wir als Modul eine Potenz der Primzahl p betrachten. Sind zwei ganze Zahlen β_1 und β_1' des Körpers $K(p, \alpha_1)$ für eine Potenz p^h von p mit ganzzahligem positivem Exponenten kongruent, so vertritt die Kongruenz:

$$\beta_1 \equiv \beta_1' \pmod{p^h}$$

eine Gleichung:

$$\beta_1 = \beta_1' + p^h \gamma_1,$$

wo γ_1 eine ganze Zahl von $K(p, \alpha_1)$ ist. Diese Gleichung bleibt richtig, wenn man zu den λ konjugierten Werten übergeht, es bestehen also die λ Gleichungen:

$$\beta_i = \beta_i' + p^h \gamma_i \qquad (i = 1, 2, \cdots \lambda),$$

und durch Multiplikation dieser λ Gleichungen ergibt sich:

$$n(\beta) = n(\beta') + p^h g_1 + p^{2h} g_2 + \cdots,$$

wo die Zahlen $g_1, g_2, \ldots$ ganze ganzzahlige symmetrische Funktionen von $(\beta_1', \ldots \beta_\lambda', \gamma_1, \ldots \gamma_\lambda)$, also ganze Zahlen von $K(p)$ sind.

X) Sind also zwei ganze algebraische Zahlen modulo p^h kongruent, so sind auch ihre Normen mindestens für denselben Modul kongruent.

Ich will nun untersuchen, welche unter den Zahlen des Körpers $K(p, \alpha)$ Einheiten sind. Schreibt man die zu untersuchende Zahl in der Form:

$$\beta = p^\varrho (\varepsilon^{(0)} + \varepsilon^{(1)} p + \cdots) = p^\varrho \gamma,$$

so erkennt man zunächst, daß $\varrho = 0$ sein muß, denn einmal darf ϱ nicht negativ sein, da ja dann β nicht algebraisch ganz sein würde. Aber ϱ darf auch nicht positiv sein, denn sonst wäre ja

$$n(\beta) = n(p^\varrho)\, n(\gamma) = p^{\lambda\varrho} \cdot G$$

keine rationale Einheit von $K(p)$, weil die Norm G der ganzen algebraischen Zahl γ auch ganz ist. Nur dann kann also die Zahl β eine Einheit sein, wenn sie die Form hat:

$$\beta = \varepsilon^{(0)} + \varepsilon^{(1)} p + \varepsilon^{(2)} p^2 + \cdots \qquad (p)$$

und die reduzierte Zahl $\varepsilon^{(0)}$ nicht Null ist. Aber nicht jede Zahl von dieser Form braucht eine Einheit zu sein. Da aber

$$\beta \equiv \varepsilon^{(0)} \pmod{p}$$

ist, so folgt nach dem soeben bewiesenen Satze X):

$$n(\beta) \equiv n(\varepsilon^{(0)}) \pmod{p},$$

d. h. $n(\beta)$ ist dann und nur dann nicht durch p teilbar, wenn dasselbe für $n(\varepsilon^{(0)})$ gilt. Daraus folgt der Satz:

XI) Eine Zahl $\beta = \varepsilon^{(0)} + \varepsilon^{(1)}p + \cdots$ ist dann und nur dann eine Einheit, wenn ihr Anfangsglied $\varepsilon^{(0)}$ eine Einheit ist.

Wir haben also, um alle algebraischen Einheiten zu finden, nur unter den p^{λ} reduzierten Zahlen

(4) $$\varepsilon = e_1\gamma^{(1)} + e_2\gamma^{(2)} + \cdots + e_\lambda\gamma^{(\lambda)} \qquad (e_k = 0, 1, \cdots p-1)$$

diejenigen auszusuchen, welche Einheiten sind, was durch die Bildung der Normen geschehen kann. Wir erhalten so ein vollständiges System modulo p inkongruenter Einheiten, und jede andere Einheit ist einer einzigen unter diesen modulo p kongruent.

§ 5. Die Primzahl des algebraischen Körpers $K(p, \alpha)$.

Ich will nun diejenigen algebraischen Zahlen β untersuchen, welche keine Einheiten sind. Da von den beiden Zahlen β und $\frac{1}{\beta}$ mindestens eine algebraisch ganz ist, so kann ich β als algebraisch ganz annehmen und voraussetzen, daß sie keine Einheit, daß also $n(\beta)$ durch p teilbar ist.

Zu diesen Zahlen β gehört auch die Primzahl p selber, da $n(p) = p^{\lambda}$ durch p teilbar ist. Aber im allgemeinen verliert die Zahl p in dem Bereiche der p-adischen algebraischen Zahlen die charakteristische Primzahleigenschaft, daß sie außer sich selbst und der Einheit keinen Teiler hat. Ist nämlich β irgend eine Zahl, deren Norm $n(\beta) = p^{b}E$ von niedrigerer Ordnung ist, als λ, so ist $\frac{p}{\beta}$ algebraisch ganz, also β ein Teiler von p; aber β ist ein eigentlicher Teiler von p, d. h. nicht äquivalent p, weil ja $\frac{\beta}{p}$ nicht ganz ist.

An die Stelle von p tritt nun, wie gleich gezeigt werden wird, als Primzahl diejenige ganze algebraische Zahl π, für welche

(1) $$n(\pi) = p^{f}E$$

von möglichst niedriger aber positiver Ordnung f ist. Eine solche Zahl π muß es geben, denn die Ordnungszahl von $n(\beta)$ ist für jede ganze algebraische Zahl β eine positive ganze Zahl oder Null und unter den positiven Ordnungszahlen muß eine die kleinste sein. Nun gibt es zwar außer π unendlich viele algebraische Zahlen, deren Norm diese kleinste positive Ordnungszahl hat, aber jede andere derartige Zahl π' ist, wie wir sahen, mit π äquivalent, unterscheidet sich also von ihr nur um eine Einheit, und umgekehrt ist auch für jede zu π äquivalente Zahl $\pi' = \pi\varepsilon$:

(1a) $$n(\pi') = n(\pi)\,n(\varepsilon) = p^{f}\bar{E}.$$

Wir wollen eine solche Zahl π oder jede mit ihr äquivalente π' die **Primzahl des Bereiches** $K(p, \alpha)$ nennen, wobei eben eine jede zu π äquivalente Primzahl π' als nicht verschieden von π angesehen wird. Die Berechtigung zu dieser Bezeichnung liefern die folgenden sehr leicht zu beweisenden Sätze:

I) Die Primzahl π besitzt im Bereiche der ganzen algebraischen Zahlen keinen eigentlichen Teiler außer den Einheiten.

Ist nämlich β eine ganze Zahl, aber keine Einheit, so ist $n(\beta)$ von höherer oder von gleicher Ordnung wie $n(\pi)$; im ersten Falle ist π ein eigentlicher Teiler von β, im zweiten Falle ist $\beta = \pi\varepsilon$.

Hieraus folgt unmittelbar der Satz:

II) Jede ganze algebraische Zahl ist entweder eine Einheit oder sie ist durch π teilbar.

Ferner besteht der Fundamentalsatz, durch welchen die charakteristische Primzahleigenschaft der Zahl π in Evidenz gesetzt wird:

III) Das Produkt zweier ganzen Zahlen ist dann und nur dann durch die Primzahl π teilbar, wenn mindestens einer der Faktoren ein Multiplum von π ist.

Ist nämlich keine der beiden ganzen Zahlen γ und γ' durch π teilbar, so sind sie nach dem vorigen Satze beide Einheiten und ihr Produkt $\gamma\gamma'$ ist mithin ebenfalls eine Einheit.

Sieht man also von den zu π äquivalenten Zahlen ab, so gibt es in dem Bereiche der algebraischen p-adischen Zahlen nur eine einzige Primzahl; nur ist diese nicht gleich p, wie dies in dem Bereiche der rationalen p-adischen Zahlen der Fall war, sondern im allgemeinen eine Zahl π, welche ein Teiler von p ist. Aber diese Primzahl π besitzt innerhalb $K(p, \alpha)$ genau dieselben Eigenschaften, wie sie p in dem Bereiche $K(p)$ zukommen. Vor allen Dingen besteht auch hier der Fundamentalsatz:

Jede ganze oder gebrochene algebraische Zahl β läßt sich auf eine einzige Weise in der Form:

IV) (2) $$\beta = \varepsilon\pi^\varrho$$

darstellen, wo ϱ eine ganze positive oder negative Zahl oder Null und ε eine Einheit unseres Bereiches bedeutet.

In der Tat, sei

$$n(\beta) = p^b \cdot E,$$

so kann man den Exponenten b stets in der Form schreiben:

$$b = \varrho f + f_0,$$

wo f_0 entweder Null oder eine der Zahlen $1, 2, \cdots f-1$ ist. Dann

sieht man sofort, daß $f_0 = 0$, also b ein Multiplum von f sein muß. Bildet man nämlich die Zahl:

$$\pi' = \frac{\beta}{\pi^\varrho},$$

so ist ja

$$n(\pi') = \frac{n(\beta)}{(n(\pi))^\varrho} = p^{b-\varrho f} \cdot E_0 = p^{f_0} E_0;$$

wäre also $f_0 > 0$, so wäre π' eine ganze Zahl unseres Bereiches, deren Norm die Ordnungszahl f_0, also eine kleinere Ordnungszahl als π hätte, und dies steht mit der über π gemachten Voraussetzung im Widerspruch. Also muß $f_0 = 0$ also

$$\pi' = \frac{\beta}{\pi^\varrho} = \varepsilon$$

eine Einheit sein. Es ist mithin in der Tat

$$\beta = \varepsilon \pi^\varrho,$$

w. z. b. w.

Auch hier will ich den ganzzahligen Exponenten ϱ die Ordnungszahl von β nennen. Ist ϱ positiv oder Null, so ist β algebraisch ganz, ist ϱ negativ, so ist β eine gebrochene Zahl. Eine Zahl β' ist dann und nur dann durch β teilbar, wenn ihre Ordnungszahl $\varrho' \geqq \varrho$ ist; beide Zahlen sind äquivalent, wenn ihre Ordnungszahlen gleich sind. Eine Zahl π' ist also nur dann ebenfalls eine Primzahl des Bereiches $K(p, \alpha)$, wenn sie die Ordnungszahl Eins hat. Ist speziell $\varrho = 0$, so ist β eine Einheit. Aus der Gleichung:

$$n(\beta) = n(\pi^\varrho \varepsilon) = p^{\varrho f} . E$$

folgt der Satz:

V) Hat die Norm der Primzahl π die Ordnungszahl f, so hat die Norm jeder p-adischen algebraischen Zahl β eine Ordnungszahl ϱf, welche gleich dem f-fachen der Ordnungszahl ϱ von β ist.

Auch die Zahl p selbst ist durch eine gewisse Potenz π^e von π genau teilbar. Aus der Gleichung:

(3) $$p = \pi^e \varepsilon$$

folgt durch Übergang zur Norm, daß $n(p) = p^\lambda = p^{ef}$, also

(3a) $$ef = \lambda$$

sein muß.

VI) Der Bereich $K(p, \alpha)$ der p-adischen algebraischen Zahlen unterscheidet sich also von dem Bereiche $K(p)$ der rationalen p-adischen Zahlen nur dadurch, daß in dem ersten p im

allgemeinen nicht selbst eine Primzahl, sondern die e^{te} Potenz einer Primzahl π ist, deren Exponent e ein genauer Teiler des Grades λ des Körpers $K(\alpha)$ ist.

Wählt man an Stelle der Primzahl π eine andere π' und beachtet, daß sich beide nur um eine Einheit unterscheiden, so erkennt man, daß die hier eingeführten Ordnungszahlen der Zahlen β, sowie die Zahl e unabhängig von der Wahl von π sind.

Da das Produkt und der Quotient zweier Einheiten wieder eine Einheit ist, so folgen aus der Multiplikation und der Division zweier Zahlen:

(4) $$\beta = \varepsilon \pi^{\varrho}, \qquad \beta' = \varepsilon' \pi^{\varrho'}$$

von den Ordnungen ϱ und ϱ' die Gleichungen:

(4a) $$\beta \beta' = \bar{\varepsilon} \pi^{\varrho + \varrho'}, \qquad \frac{\beta}{\beta'} = \bar{\bar{\varepsilon}} \pi^{\varrho - \varrho'},$$

wo $\bar{\varepsilon}$ und $\bar{\bar{\varepsilon}}$ wieder Einheiten sind.

VII) Die Ordnungszahl des Produktes bzw. des Quotienten zweier Zahlen unseres Bereiches ist also gleich der Summe bzw. gleich der Differenz der Ordnungen jener Zahlen.

Da die Zahl Null die Ordnungszahl Unendlich hat, so gilt auch für das Gebiet der p-adischen algebraischen Zahlen der Fundamentalsatz der multiplikativen Zahlentheorie:

VIII) Das Produkt zweier Zahlen ist dann und nur dann gleich Null, wenn mindestens einer der Faktoren Null ist.

Es ist nun sehr leicht, durch eine endliche Anzahl von Versuchen einen Primteiler π des Bereiches $K(p, \alpha)$ auszuwählen, und zwar kann man ihn, wenn man will, so aussuchen, daß er eine ganze algebraische Zahl des engeren Bereiches $K(\alpha)$ ist.

Eine ganze Zahl des Bereiches $K(p, \alpha)$ ist ja nämlich dann und nur dann eine solche Primzahl, wenn sie in allen denjenigen ganzen algebraischen Zahlen

(5) $$\gamma = \varepsilon^{(0)} + \varepsilon^{(1)} p + \cdots$$

desselben Bereiches enthalten ist, welche nicht Einheiten sind, d. h. in allen denen, für welche das Anfangsglied $\varepsilon^{(0)}$ keine Einheit ist.

Sind nun zuerst alle $p^{\lambda} - 1$ modulo p reduzierten Zahlen

(6) $$\varepsilon^{(0)} = e_1 \gamma^{(1)} + e_2 \gamma^{(2)} + \cdots + e_{\lambda} \gamma^{(\lambda)} \qquad (e_i = 0, 1, \cdots p - 1)$$

außer der Zahl Null Einheiten, und davon kann man sich durch die Bildung der Normen $n(\varepsilon^{(0)})$ überzeugen, so ist p selbst in dem Körper $K(p, \alpha)$ eine Primzahl, denn für jede Zahl γ in (5) ist ja

(7) $$\gamma \equiv \varepsilon^{(0)} \pmod{p}$$

d. h. p ist in jeder ganzen Zahl γ enthalten, für welche das Anfangsglied gleich Null, welche also keine Einheit ist.

Sind dagegen nicht alle reduzierten Zahlen $\varepsilon^{(0)}$ Einheiten, und ist $\pi^{(0)}$ unter ihnen so gewählt, daß ihre Norm eine möglichst kleine aber positive Ordnungszahl hat, so ist, eben wegen dieser Eigenschaft, $\pi^{(0)}$ ein Teiler aller modulo p reduzierten Zahlen $\varepsilon^{(0)}$, welche keine Einheiten sind; außerdem ist $\pi^{(0)}$ aber auch ein Teiler von p, denn von den beiden Zahlen $\frac{\pi^{(0)}}{p}$ und $\frac{p}{\pi^{(0)}}$ muß ja nach (I) a. S. 134 eine ganz sein, und die erste könnte nur ganz sein, wenn die reduzierte Zahl $\pi^{(0)}$ durch p teilbar wäre, wenn also alle Koeffizienten e_i von $\pi^{(0)}$ gleich Null sind.

Somit besteht also auch modulo $\pi^{(0)}$ für jede Zahl γ in (5) die Kongruenz:

$$\gamma \equiv \varepsilon^{(0)}, \quad (\text{mod}\, \pi^{(0)}),$$

und da, falls $\varepsilon^{(0)}$ keine Einheit ist, $\varepsilon^{(0)}$ ein Multiplum von $\pi^{(0)}$ ist, so ist wirklich jede Zahl γ, welche keine Einheit ist, ein Multiplum von $\pi^{(0)}$, d. h. $\pi^{(0)}$ ist wirklich die Primzahl unseres Bereiches.

IX) In dem Körper $K(p, \alpha)$ ist also diejenige modulo p reduzierte Zahl

$$\pi^{(0)} = e_1\gamma^{(1)} + e_2\gamma^{(2)} + \cdots + e_\lambda\gamma^{(\lambda)}$$

eine Primzahl, deren Norm von der niedrigsten aber positiven Ordnung ist. Sind aber alle diese reduzierten Zahlen Einheiten, so ist p selbst auch in dem Bereiche $K(p, \alpha)$ eine Primzahl.

Man kann also die Primzahl π in dem Bereiche $K(p, \alpha)$ stets durch eine endliche Anzahl von Versuchen finden, und zwar so, daß sie eine absolut ganze algebraische Zahl des engeren Bereiches $K(\alpha)$ ist.

§ 6. Der Primteiler $\mathfrak{p}$ des Körpers $K(p, \alpha)$.

In dem Bereiche $K(p, \alpha)$ existieren unendlich viele Primzahlen $\pi, \pi', \ldots$, aber sie können für alle Fragen der Division durch eine unter ihnen ersetzt werden, da sich ja alle anderen von dieser nur durch je eine Einheit unterscheiden, welche (wegen S. 137 (IX)) für alle Fragen der Teilbarkeit vollständig unwesentlich ist, deren geeignete Wahl aber bei den späteren eingehenderen Untersuchungen von Wichtigkeit sein wird.

Um nun nicht immer von diesen verschiedenen aber äquivalenten Primzahlen sprechen zu müssen, will ich dem Bereiche $K(p, \alpha)$ von vorn herein einen einzigen Primdivisor oder Primteiler $\mathfrak{p}$ zuordnen,

und ich will die Teilbarkeit einer Zahl durch eine Potenz von $\mathfrak{p}$ folgendermaßen einfach definieren:

Eine ganze oder gebrochene Zahl β ist durch die ϱ^{te} Potenz $\mathfrak{p}^\varrho$ von $\mathfrak{p}$ **genau teilbar**, wenn β die Ordnungszahl ϱ besitzt, wenn also für jede der äquivalenten Primzahlen π des Bereiches $K(p, \alpha)$:

$$\beta = \varepsilon \pi^\varrho$$

ist, wo ε eine Einheit bedeutet.

Allgemeiner heißt eine Zahl β durch $\mathfrak{p}^{\varrho_0}$ **teilbar**, wenn ihre Ordnungszahl $\varrho \geqq \varrho_0$ ist, wenn also β durch die ϱ_0^{te}, aber eventuell auch durch eine höhere Potenz irgend einer Primzahl π algebraisch teilbar ist. Wir wollen diese letzte Tatsache durch die Kongruenz

$$\beta \equiv 0 \pmod{\mathfrak{p}^{\varrho_0}}$$

ausdrücken. Sie vertritt die Kongruenz:

$$\beta \equiv 0, \pmod{\pi^{\varrho_0}},$$

wo π jede der äquivalenten Primzahlen bezeichnen kann.

Allgemeiner heißen zwei Zahlen β und β' **modulo** $\mathfrak{p}^{\varrho_0}$ **kongruent**, wenn ihre Differenz durch $\mathfrak{p}^{\varrho_0}$ teilbar ist; wir drücken diese Tatsache durch die Kongruenz:

$$\beta \equiv \beta' \pmod{\mathfrak{p}^{\varrho_0}}$$

aus.

Jede Zahl β ist durch eine bestimmte Potenz $\mathfrak{p}^\varrho$ von $\mathfrak{p}$ genau teilbar, deren Exponent gleich der Ordnungszahl von β ist. Sind β und β' genau durch $\mathfrak{p}^\varrho$ und $\mathfrak{p}^{\varrho'}$ teilbar, so ist ihr Produkt $\beta\beta'$ und ihr Quotient $\frac{\beta}{\beta'}$ genau bzw. durch $\mathfrak{p}^{\varrho+\varrho'}$ und $\mathfrak{p}^{\varrho-\varrho'}$ genau teilbar.

Unter der **Norm des Divisors** $\mathfrak{p}$ will ich die Potenz p^f der Primzahl p verstehen, durch welche die Norm $n(\pi)$ einer jeden Primzahl π von $K(p, \alpha)$ genau teilbar ist. Ich nenne dann f den **Grad des Divisors** $\mathfrak{p}$. Allgemeiner setze ich

(1) $$n(\mathfrak{p}^\varrho) = (n(\mathfrak{p}))^\varrho = p^{\varrho f}$$

gleich der in den Normen der Potenzen π^ϱ aller Primzahlen π enthaltenen Potenz von p. Ist dann eine Zahl β genau durch $\mathfrak{p}^\varrho$ teilbar, so ist ihre Norm genau durch $n(\mathfrak{p}^\varrho)$ teilbar.

Ist die reelle Primzahl p genau durch $\mathfrak{p}^e$ teilbar, wie wir dies vorher angenommen haben, so soll e die **Ordnung des Primdivisors** $\mathfrak{p}$ genannt werden. Da $ef = \lambda$ ist, so ist stets das Produkt aus dem Grade

und der Ordnung eines Primdivisors $\mathfrak{p}$ gleich dem Grade des Körpers $K(p, \alpha)$.

Ich wende mich jetzt zu einer genaueren Untersuchung der Zahlen des Bereiches $K(p, \alpha)$ für eine beliebige Potenz des zugehörigen Primteilers $\mathfrak{p}$ als Modul, und ich betrachte da zuerst die ganzen algebraischen Zahlen dieses Bereiches für den Modul $\mathfrak{p}$ selbst.

Jede ganze Zahl $\gamma = \varepsilon^{(0)} + \varepsilon^{(1)}p + \dots$ ist modulo p einer einzigen reduzierten Zahl $\varepsilon^{(0)}$, d. h. einer unter den p^λ ganzen algebraischen Zahlen

(2) $$\varepsilon^{(0)} = e_1\gamma^{(1)} + e_2\gamma^{(2)} + \cdots + e_\lambda\gamma^{(\lambda)} \quad (e_i = 0, 1, \cdots p-1)$$

kongruent, und da p genau durch $\mathfrak{p}^e$ teilbar ist, so bleibt die Kongruenz

(2a) $$\gamma \equiv \varepsilon^{(0)} \pmod{\mathfrak{p}^e}$$

auch bestehen, wenn man den Modul $\mathfrak{p}^e$ durch seinen Teiler $\mathfrak{p}$ ersetzt. Aber die p^λ modulo p, oder, was dasselbe ist, modulo $\mathfrak{p}^e$ reduzierten Zahlen $\varepsilon^{(0)}$ brauchen modulo $\mathfrak{p}$ nicht alle inkongruent zu sein, obwohl sie es modulo $\mathfrak{p}^e$ sind. Jedoch kann man aus diesen p^λ Zahlen (2) sehr leicht ein vollständiges System modulo $\mathfrak{p}$ inkongruenter Zahlen dadurch herleiten, daß man von allen untereinander modulo $\mathfrak{p}$ kongruenten Zahlen $\varepsilon^{(0)}, \varepsilon^{(0)'}, \dots$, dieser Reihe immer nur je eine beibehält.

Es mögen nun die σ ganzen algebraischen Zahlen

(2b) $$\overset{(0)}{\varepsilon}, \overset{(1)}{\varepsilon}, \dots \overset{(\sigma-1)}{\varepsilon}$$

diejenigen unter jenen p^λ modulo p reduzierten Zahlen sein, welche ein vollständiges System modulo $\mathfrak{p}$ inkongruenter Zahlen bilden. Dann ist nur eine unter ihnen durch π teilbar, und für sie kann die Zahl Null gewählt werden; alle $\sigma - 1$ anderen sind Einheiten modulo $\mathfrak{p}$. Irgend eine ganze Zahl β ist dann modulo $\mathfrak{p}$ einer und nur einer dieser σ Zahlen kongruent. Ich sage dann, die σ Zahlen (2b) bilden ein vollständiges Restsystem modulo $\mathfrak{p}$.

Es sei nun π irgend eine beliebig, aber fest gewählte Primzahl des Bereiches $K(p, \alpha)$; dann ergibt sich für eine beliebige ganze Zahl β die Kongruenz:

(3) $$\beta \equiv \varepsilon^{(0)} \pmod{\mathfrak{p}}$$

und diese vertritt eine Gleichung:

(3a) $$\beta = \varepsilon^{(0)} + \pi\beta^{(1)},$$

wo $\varepsilon^{(0)}$ eine der obigen σ Zahlen (2b) und $\beta^{(1)}$ wieder eine bestimmte ganze Zahl bedeutet. Schreibt man $\beta^{(1)}$ in derselben Weise und fährt so fort, so erhält man wie a. S. 124 (4) und (4a) eine beliebig weit auszudehnende Reihe linearer Gleichungen:

(3b)
$$\begin{aligned} \beta &= \varepsilon^{(0)} + \pi\beta^{(1)}, \\ \beta^{(1)} &= \varepsilon^{(1)} + \pi\beta^{(2)}, \\ &\cdots\cdots \\ &\cdots\cdots \\ \beta^{(k)} &= \varepsilon^{(k)} + \pi\beta^{(k+1)}, \\ &\cdots\cdots \end{aligned}$$

Multipliziert man nun diese Gleichungen der Reihe nach mit $1, \pi, \ldots, \pi^k \ldots$, addiert sie und läßt die rechts und links gleichzeitig auftretenden Glieder $\beta^{(i)}\pi^i$ weg, so erhält man für β die folgende eindeutig bestimmte Darstellung für den Bereich von $\mathfrak{p}$:

(4) $$\beta = \varepsilon^{(0)} + \varepsilon^{(1)}\pi + \varepsilon^{(2)}\pi^2 + \cdots \quad (p),$$

oder wenn wir jetzt für die nach Potenzen von π fortschreitende Reihe die abgekürzte Schreibweise anwenden:

(4a) $$\beta = \varepsilon^{(0)}, \varepsilon^{(1)}\varepsilon^{(2)}\ldots \quad (p).$$

Die beiden letzten Gleichungen sind wieder so aufzufassen, daß β durch die beliebig weit fortgesetzte Reihe auf der rechten Seite mit jeder vorgegebenen Genauigkeit bestimmt werden kann in dem Sinne, daß die Näherungswerte

$$\beta^{(k)} = \varepsilon^{(0)}, \varepsilon^{(1)}\ldots\varepsilon^{(k)}$$

für jedes noch so große k der Zahl β kongruent sind modulo $\mathfrak{p}^{k+1}$.

Um allgemeiner eine Zahl $\beta = \pi^\varrho\varepsilon$ von der positiven oder negativen Ordnung ϱ darzustellen, habe ich nur noch jedes Glied der obigen Entwicklung mit π^ϱ zu multiplizieren, d. h. das Komma um ϱ Stellen nach rechts oder links zu verschieben, je nachdem ϱ positiv oder negativ ist. Es ergibt sich also der folgende wichtige Satz:

Jede p-adische Zahl des Körpers $K(p, \alpha)$, also auch speziell jede algebraische Zahl des Körpers $K(\alpha)$ läßt sich für den Bereich von p auf eine einzige Weise in der Form darstellen:

$$\beta = \varepsilon^{(\varrho)}\pi^\varrho + \varepsilon^{(\varrho+1)}\pi^{\varrho+1} + \cdots \quad (p),$$

wo die Koeffizienten $\varepsilon^{(i)}$ eindeutig bestimmte Zahlen des Systems $(\overset{(0)}{\varepsilon}, \overset{(1)}{\varepsilon}, \ldots \overset{(\sigma-1)}{\varepsilon})$ sind, und π einen Primfaktor von p für den Bereich $K(\alpha)$ bedeutet.

Es ist jetzt leicht, die Anzahl σ der modulo $\mathfrak{p}$ inkongruenten reduzierten ganzen Zahlen $\overset{(i)}{\varepsilon}$ in (2b) zu finden. Zu diesem Zwecke bilde ich auf zwei verschiedene Weisen ein vollständiges System von modulo $p \sim \mathfrak{p}^e$ inkongruenten ganzen algebraischen Zahlen des Körpers $K(\alpha)$. Erstens ist ein solches gegeben durch die p^λ Zahlen:

$$l_1\gamma^{(1)} + l_2\gamma^{(2)} + \cdots + l_\lambda\gamma^{(\lambda)} \qquad (l_i = 0, 1, \cdots p-1),$$

(s. S. 124 oben), zweitens bilden auch die Zahlen:

$$\varepsilon^{(0)} + \varepsilon^{(1)}\pi + \cdots + \varepsilon^{(e-1)}\pi^{e-1}$$

ein vollständiges System modulo $\mathfrak{p}^e \sim p$ inkongruenter ganzer Zahlen, wenn man jede der Zahlen $\varepsilon^{(i)}$ ein vollständiges Restsystem $(\overset{(0)}{\varepsilon}, \overset{(1)}{\varepsilon}, \ldots \overset{(\sigma-1)}{\varepsilon})$ modulo $\mathfrak{p}$ durchlaufen läßt. Da die Anzahl der inkongruenten Zahlen in beiden Systemen dieselbe ist, so muß

$$\sigma^e = p^\lambda = p^{ef}, \quad \text{d. h.} \quad \sigma = p^f = n(\mathfrak{p})$$

sein. Es besteht also der Satz:

> Die Anzahl aller modulo $\mathfrak{p}$ inkongruenten Zahlen des Körpers $K(\alpha)$ ist der Norm jenes Primteilers $\mathfrak{p}$ gleich.

Beachtet man ferner, daß offenbar die $p^{\varrho f}$ Zahlen

$$\varepsilon^{(0)} + \varepsilon^{(1)}\pi + \cdots + \varepsilon^{(\varrho-1)}\pi^{\varrho-1}$$

ein vollständiges System von modulo $\mathfrak{p}^\varrho$ inkongruenten ganzen algebraischen Zahlen bilden, wenn man jeden der ϱ Koeffizienten $\varepsilon^{(i)}$ unabhängig von den anderen das vollständige Restsystem (2b) durchlaufen läßt, so ergibt sich der allgemeinere Satz:

> Die Anzahl aller modulo $\mathfrak{p}^\varrho$ inkongruenten ganzen algebraischen Zahlen des Körpers $K(\alpha)$ ist gleich der Norm $n(\mathfrak{p}^\varrho)$ dieses Divisors.

§ 7. Die konjugierten Körper und die konjugierten Entwicklungen für den Bereich von $\mathfrak{p}$.

Bei den bis jetzt durchgeführten Untersuchungen wurde ein beliebiger Körper $K(\alpha)$ unter den λ konjugierten:

$$K(\alpha_1),\ K(\alpha_2), \ldots K(\alpha_\lambda)$$

zu Grunde gelegt. Man erkennt aber, daß die für ihn gefundenen Resultate ohne jede Änderung für alle diese konjugierten Körper gültig bleiben.

Eine ganze Zahl π_1 in dem Körper $K(\alpha_1)$ ist ja dadurch als Primzahl charakterisiert, daß ihre Norm:

(1) $$n(\pi) = \pi_1\,\pi_2 \cdots \pi_\lambda = p^f E$$

keine Einheit und von möglichst niedriger Ordnung in p ist. Ebenso ist eine Einheit ε_1 von $K(\alpha_1)$ allein dadurch charakterisiert, daß ihre Norm eine Einheit modulo p ist. Ist also eine Zahl von $K(\alpha_1)$ eine Primzahl, bzw. eine Einheit, so gilt das Entsprechende für alle ihre Konjugierten. Allgemeiner bleibt jede Kongruenz:

(2) $$\beta_1 \equiv \beta_1' \pmod{\pi_1^\varrho}$$

für eine beliebige Potenz von π_1 als Modul richtig, wenn man zu den konjugierten Körpern übergeht; aus ihr folgen also die λ konjugierten Kongruenzen:

(2a) $$\beta_i \equiv \beta_i' \pmod{\pi_i^\delta} \qquad (i = 1, 2, \cdots \lambda),$$

denn sie vertreten ja die Gleichungen:

(2b) $$\beta_i = \beta_i' + \pi_i^\delta \gamma_i \qquad (i = 1, 2, \cdots \lambda),$$

in denen die γ_i ganze algebraische Zahlen der Körper $K(\alpha_i)$ sind, und von diesen λ Gleichungen ist ja jede eine notwendige Folge der anderen. Wir erhalten also den folgenden Satz:

Ist π_1 in dem Körper $K(\alpha_1)$ eine Primzahl, so sind die λ konjugierten Zahlen $\pi_1, \pi_2, \ldots \pi_\lambda$ in den λ konjugierten Körpern $K(\alpha_1), K(\alpha_2), \ldots K(\alpha_\lambda)$ bzw. ebenfalls Primzahlen. Alle diese konjugierten Primzahlen haben dieselbe Ordnung e und denselben Grad f. Ist β_1 irgend eine Zahl von $K(\alpha_1)$, deren Ordnungszahl ϱ ist, so besitzen alle konjugierten Zahlen β_i dieselbe Ordnungszahl. Bilden

$$\overset{(0)}{\varepsilon_1}, \overset{(1)}{\varepsilon_1}, \ldots \overset{(\sigma-1)}{\varepsilon_1}$$

ein vollständiges System modulo π_1 inkongruenter ganzer Zahlen des Bereiches $K(\alpha_1)$, so bilden allgemein die σ konjugierten Zahlen des Bereiches $K(\alpha_i)$

$$\overset{(0)}{\varepsilon_i}, \overset{(1)}{\varepsilon_i}, \ldots \overset{(\sigma-1)}{\varepsilon_i}$$

ein vollständiges System modulo π_i inkongruenter Zahlen für diesen Bereich.

Ist β_1 irgend eine Zahl des Körpers $K(\alpha_1)$, so besteht nach dem a. S. 145 bewiesenen Satze eine Darstellung von der folgenden Form:

(3) $$\beta_1 = \varepsilon_1^{(\varrho)} \pi_1^\varrho + \varepsilon_1^{(\varrho+1)} \pi_1^{\varrho+1} + \cdots \quad (p),$$

und da jede Gleichung innerhalb dieses Bereiches beim Übergang zu den konjugierten Zahlen richtig bleibt, so ergeben sich aus ihr die folgenden λ Darstellungen der konjugierten Zahlen $\beta_1, \beta_2, \ldots \beta_\lambda$:

(3a) $$\beta_i = \varepsilon_i^{(\varrho)} \pi_i^\varrho + \varepsilon_i^{(\varrho+1)} \pi_i^{\varrho+1} + \cdots \quad (p) \qquad (i = 1, 2, \cdots \lambda).$$

Diese konjugierten Wurzeln bilden also einen Zyklus von λ konjugierten p-adischen algebraischen Zahlen, welche nach ganzen Potenzen der konjugierten Primzahlen π_i fortschreiten.

Wir werden nun sehr bald sehen, daß im allgemeinen die gemeinsame Ordnung e dieser Primzahlen π_i gleich Eins ist, d. h. daß im allgemeinen

$$\pi_1 = \pi_2 = \cdots = \pi_\lambda = p$$

angenommen werden kann; dann bilden also die λ konjugierten Zahlen β_i einen Zyklus p-adischer Zahlen, welche alle nach ganzen Potenzen der

Primzahl p fortschreiten; diese unterscheiden sich also allein dadurch von den **rationalen** p-adischen Zahlen

$$e^{(\varrho)} p^{\varrho} + e^{(\varrho+1)} p^{\varrho+1} + \cdots,$$

daß die Koeffizienten $\varepsilon_i^{(r)}$ eindeutig bestimmte Zahlen aus der Reihe $(\overset{(0)}{\varepsilon_i}, \overset{(1)}{\varepsilon_i}, \ldots \overset{(\sigma-1)}{\varepsilon_i})$ aller p^f modulo $\mathfrak{p}$ inkongruenten ganzen Zahlen des Bereiches $K(\alpha_i)$ sind, während die $e^{(r)}$ eindeutig bestimmte Zahlen aus der Reihe $(0, 1, \ldots p-1)$ aller p modulo p inkongruenten ganzen Zahlen des Bereiches $K(1)$ waren. Nur in gewissen, besonderen Fällen, welche aber stets auftreten können, sind diese λ konjugierten Primzalhen π_i nicht gleich p, sondern es ist dann:

(4) $$p = \pi_i^e \bar{\varepsilon}_i,$$

wo $\bar{\varepsilon}_i$ eine Einheit bedeutet, oder also es sind die λ konjugierten Primzahlen $\pi_1, \pi_2, \ldots \pi_\lambda$ Wurzeln der Gleichungen e^{ten} Grades

(4a) $$\pi_i^e = p\, \varepsilon_i,$$

wenn allgemein $\varepsilon_i = \frac{1}{\bar{\varepsilon}_i}$ wieder eine Einheit von $K(\alpha_i)$ ist.

Also ist in diesem allgemeinsten Falle:

(4b) $$\pi_i = p^{\frac{1}{e}} \overset{(0)}{\varepsilon_i}$$

wo $\overset{(0)}{\varepsilon_i} = \sqrt[e]{\varepsilon_i}$ zwar im allgemeinen nicht mehr dem Körper $K(p, \alpha_i)$ angehört, aber doch eine algebraische Einheit modulo p ist, weil ja ihre e^{te} Potenz gleich ε_i, also eine Einheit ist (vgl. d. Bem. a. S. 135 unten). Aber man sieht, daß auch allgemeiner die konjugierten Primzahlen $\pi_1, \pi_2, \ldots \pi_\lambda$ alle untereinander äquivalent sind, da sie sich nur um Einheiten unterscheiden, welche allerdings im allgemeinen keinem der Körper $K(\alpha_i)$ angehören. In der Tat folgt ja aus den Gleichungen:

$$\pi_i^e = p\varepsilon_i, \qquad \pi_k^e = p\,\varepsilon_k,$$

daß

$$\left(\frac{\pi_i}{\pi_k}\right)^e = \frac{\varepsilon_i}{\varepsilon_k} = \varepsilon_{ik}$$

ist, wo auch ε_{ik} als Quotient der beiden Einheiten ε_i und ε_k eine Einheit sein muß; also ist

$$\frac{\pi_i}{\pi_k} = \sqrt[e]{\varepsilon_{ik}} = \overset{(0)}{\varepsilon_{ik}},$$

und $\overset{(0)}{\varepsilon_{ik}}$ ist wieder eine Einheit. Also ist

(5) $$\pi_i = \pi_k \overset{(0)}{\varepsilon_{ik}},$$

beide Primteiler sind also wirklich äquivalent, und beide sind nach (4b) äquivalent $p^{\frac{1}{e}}$.

In diesem Falle sind demnach die λ konjugierten Primzahlen π_i nicht gleich p, sondern, abgesehen von Einheiten, gleich $p^{\frac{1}{e}}$, und die konjugierten Reihenentwicklungen (3a) schreiten also nicht nach ganzen Potenzen der Primzahl p selbst, sondern nach ganzen Potenzen von $p^{\frac{1}{e}}$ fort. Der hier auftretende Zyklus konjugierter p-adischer Zahlen hat also ganz ähnlichen Charakter wie der Zyklus der konjugierten Potenzreihen:

$$u = \varepsilon^{(\varrho)}(z-\alpha)^{\frac{\varrho}{e}} + \varepsilon^{(\varrho+1)}(z-\alpha)^{\frac{\varrho+1}{e}} + \cdots$$

für die Wurzeln u einer algebraischen Gleichung $f(u, z) = 0$ in der Umgebung eines e-blättrigen Verzweigungspunktes $(z = \alpha)$. Daß dieses Entsprechen keine bloße Analogie ist, sondern daß jene beiden Theorieen auch hier in Wahrheit völlig identisch sind, wird später gezeigt werden.

Wir wollen aber mit Rücksicht auf diese Beziehung die Zahl p eine Verzweigungszahl e^{ter} Ordnung für den Körper $K(\alpha)$ nennen, wenn p die e^{te} Potenz einer Primzahl π ist. Ist $e = 1$, also p selbst eine Primzahl innerhalb $K(\alpha)$, so soll p eine Verzweigungszahl erster Ordnung oder eine reguläre Primzahl für den Bereich $K(\alpha)$ genannt werden.

Da alle Resultate, welche sich auf die Teilbarkeit der Zahlen β_i durch eine Potenz einer Primzahl π_i des Körpers $K(\alpha_i)$ beziehen, eine notwendige Folge der entsprechenden Tatsachen innerhalb eines dieser Körper $K(\alpha_1)$ sind, und da alle konjugierten Primzahlen $\pi_1, \pi_2, \ldots \pi_\lambda$ untereinander äquivalent sind, so will ich im folgenden den Ausdruck der hier auftretenden Teilbarkeitsbeziehungen dadurch erleichtern, daß ich allen λ konjugierten Körpern denselben Primteiler $\mathfrak{p}$ zuordne, und ich will jetzt die Teilbarkeit einer algebraischen Zahl durch eine Potenz von $\mathfrak{p}$ folgendermaßen definieren:

Eine Zahl β des Bereiches $K(\alpha)$ ist durch $\mathfrak{p}^\varrho$ genau teilbar, wenn jede der λ konjugierten Zahlen β_i genau die Ordnungszahl ϱ besitzt, wenn also

$$\beta_i = \varepsilon_i \pi_i^\varrho \qquad (i = 1, 2, \cdots \lambda)$$

ist, wo π_i eine Primzahl von $K(\alpha_i)$ bedeutet, und ε_i eine Einheit jenes Körpers ist.

Eine Zahl β ist allgemeiner durch $\mathfrak{p}^{\varrho_0}$ teilbar, oder sie genügt der Kongruenz:

(5) $$\beta \equiv 0 \pmod{\mathfrak{p}^{\varrho_0}}.$$

wenn jede der λ konjugierten Zahlen β_i durch die ϱ_0^{te}, aber eventuell auch durch eine höhere Potenz einer Primzahl π_i

des zugehörigen Körpers $K(\alpha_i)$ teilbar ist. Sie vertritt also jede der λ Kongruenzen:

(5 a) $$\beta_i \equiv 0 \pmod{\pi_i^{\varrho_0}} \qquad (i = 1, 2, \cdots \lambda).$$

Die vorher gegebenen Definitionen der Ordnung, des Grades und der Norm des Primteilers $\mathfrak{p}$ behalten ihre Gültigkeit. Zwei Zahlen β und β' heißen **kongruent modulo** $\mathfrak{p}^\varrho$, wenn die Kongruenz:

$$\beta_i \equiv \beta_i' \pmod{\pi_i^\varrho}$$

für einen der λ konjugierten Körper $K(\alpha_1), \ldots K(\alpha_\lambda)$ und somit auch für alle besteht. Zwei Zahlen β und β' sollen **gleich für den Bereich von** $\mathfrak{p}$ (oder für den Bereich von p) heißen, wenn sie für jede noch so hohe Potenz von $\mathfrak{p}$ (oder, was dasselbe ist, von p) kongruent sind (s. S. 128 oben). Diese Beziehung werde durch die Gleichung

$$\beta = \beta' \quad (\mathfrak{p})$$

ausgedrückt.

Die λ konjugierten p-adischen algebraischen Zahlen

$$\beta_1, \beta_2, \ldots \beta_\lambda$$

lassen sich für den Bereich von $\mathfrak{p}$ in konjugierte Reihen

$$\beta_i = \sum_{\nu=\varrho}^{\infty} \varepsilon_i^{(\nu)} \pi_i^\nu \quad (\mathfrak{p}) \qquad (i = 1, 2, \cdots \lambda)$$

entwickeln, welche nach ganzen Potenzen irgendwelcher konjugierten Primzahlen π_i der Bereiche $K(\alpha_i)$ fortschreiten; ich will diese λ Entwicklungen gemeinsam **die dem Primteiler $\mathfrak{p}$ zugeordneten p-adischen Darstellungen von β** nennen.

Sind allgemeiner:

(6) $$\beta_1 = \varepsilon_1 \pi_1^\varrho, \qquad \gamma_2 = \zeta_2 \pi_2^\sigma$$

zwei Zahlen der beiden konjugierten Körper $K(\alpha_1)$ und $K(\alpha_2)$, welche bzw. genau durch $\mathfrak{p}^\varrho$ und $\mathfrak{p}^\sigma$ teilbar sind, und beachtet man, daß die beiden konjugierten Primzahlen π_1 und π_2 äquivalent sind, daß also:

(6 a) $$\pi_2 = \varepsilon_{12} \pi_1$$

ist, wo ε_{12} auch eine Einheit bedeutet, so folgt aus den Gleichungen:

$$\beta_1 \gamma_2 = \varepsilon_1 \zeta_2 \cdot \pi_1^\varrho \pi_2^\sigma = \left(\varepsilon_1 \zeta_2 \varepsilon_{12}^\sigma\right) \pi_1^{\varrho+\sigma},$$

(6 b) $$\frac{\beta_1}{\gamma_2} = \frac{\varepsilon_1}{\zeta_2 \varepsilon_{12}^\sigma} \pi_1^{\varrho-\sigma},$$

$$\beta_1 \pm \gamma_2 = \pi_1^\varrho \left(\varepsilon_1 \pm \zeta_2 \varepsilon_{12}^\sigma \pi_1^{\sigma-\varrho}\right),$$

daß das Produkt und der Quotient jener Zahlen bzw. genau durch $\mathfrak{p}^{\varrho+\sigma}$ und $\mathfrak{p}^{\varrho-\sigma}$ teilbar ist; ferner folgt aus der dritten Gleichung, daß die Summe oder die Differenz zweier Zahlen von den Ordnungen ϱ und σ

mindestens durch $\mathfrak{p}^\varrho$ teilbar ist, wenn $\varrho \leq \sigma$ ist. Also behält auch für diejenigen p-adischen algebraischen Zahlen, welche aus Zahlen verschiedener konjugierter Körper durch die elementaren Rechenoperationen zusammengesetzt sind, $\mathfrak{p}$ ebenfalls den Charakter eines Primteilers.

Ich will diese Resultate benutzen, um gleich hier einen der wichtigsten Sätze unserer Theorie zu beweisen. Bis jetzt hat sich nämlich ergeben, daß die einem Primteiler $\mathfrak{p}$ zugeordneten Reihen nach ganzen Potenzen der konjugierten algebraischen Zahlen

$$\pi_i = p^{\frac{1}{e}} \varepsilon_i ,$$

d. h. im allgemeinen nach gebrochenen Potenzen der Primzahl p fortschreiten. In den allermeisten Fällen ist aber wie bereits a. S. 147 unten erwähnt wurde, der Nenner e des Exponenten gleich Eins, d. h. es ist

$$\pi_1 = \pi_2 = \cdots = \pi_\lambda = p,$$

und jene konjugierten algebraischen Zahlen β_i schreiten ebenso wie die rationalen p-adischen Zahlen nach ganzen Potenzen von p fort, allerdings mit algebraischen Koeffizienten. Es besteht nämlich der Satz:

Ist die Körperdiskriminante $d(\gamma^{(1)}, \ldots \gamma^{(\lambda)})$ von $K(\alpha)$ durch p nicht teilbar, so ist p selber in diesem Körper eine Primzahl.

Dieser Satz ist offenbar vollständig bewiesen, wenn die Richtigkeit des folgenden Theorems dargetan ist:

Ist $(\gamma_1^{(1)}, \gamma_1^{(2)}, \ldots \gamma_1^{(\lambda)})$ ein Fundamentalsystem für den Körper $K(\alpha_1)$, dessen Diskriminante durch p nicht teilbar ist, so ist eine ganze Zahl

$$\beta_1 = c_1 \gamma_1^{(1)} + c_2 \gamma_1^{(2)} + \cdots + c_\lambda \gamma_1^{(\lambda)} \tag{7}$$

dann und nur dann durch den Primteiler $\mathfrak{p}$ teilbar, wenn sie durch die reelle Primzahl p teilbar ist.

Aus diesem Satze folgt nämlich, daß eine ganze Zahl π_1, deren Norm von positiver, aber möglichst niedriger Ordnung ist, genau durch p selbst teilbar sein muß.

Soll nun β_1 in (7) durch $\mathfrak{p}$ teilbar sein, so gilt dasselbe auch für die konjugierten Zahlen $\beta_2, \ldots \beta_\lambda$. Also müssen $c_1, c_2, \ldots c_\lambda$ so bestimmt werden, daß sie den λ linearen Kongruenzen:

$$\begin{aligned} c_1 \gamma_1^{(1)} + \cdots + c_\lambda \gamma_1^{(\lambda)} &\equiv 0 \\ c_1 \gamma_2^{(1)} + \cdots + c_\lambda \gamma_2^{(\lambda)} &\equiv 0 \\ &\vdots \\ c_1 \gamma_\lambda^{(1)} + \cdots + c_\lambda \gamma_\lambda^{(\lambda)} &\equiv 0 \end{aligned} \pmod{\mathfrak{p}} \tag{7a}$$

genügen, deren Auflösung die λ Bedingungen:

$$c_h \cdot \left| \gamma_k^{(i)} \right| \equiv 0 \pmod{\mathfrak{p}} \qquad (h = 1, 2, \cdots \lambda) \tag{7b}$$

ergibt. Ist nun, wie vorausgesetzt wurde, die Diskriminante

$$d(\gamma^{(1)}, \dots \gamma^{(\lambda)}) = |\gamma_k^{(i)}|^2$$

eine Einheit modulo p, so müssen wegen (7 b) alle Koeffizienten $c_1, c_2, \dots c_\lambda$ durch $\mathfrak{p}$ teilbar sein; da diese aber rationale ganze Zahlen sind, so können sie nur dann $\mathfrak{p}$ enthalten, wenn sie alle durch p teilbar sind, wenn also allgemein $c_k = p\bar{c}_k$, mithin:

$$\beta = p(\bar{c}_1\gamma^{(1)} + \cdots + \bar{c}_\lambda\gamma^{(\lambda)})$$

ist. Dann ist aber β algebraisch durch p teilbar, unsere Behauptung ist also vollständig bewiesen. Erst später werde ich zeigen, daß auch umgekehrt, falls die Körperdiskriminante durch p teilbar ist, p in diesem Körper den Primzahlcharakter verliert; es wird eine besonders wichtige Aufgabe sein, die Ordnungszahl der Körperdiskriminante zu bestimmen, wenn die Ordnungszahl e des Primfaktors $\pi \sim p^{\frac{1}{e}}$ gegeben ist.

Der hier betrachtete einfachste Fall tritt sicher ein, wenn die Diskriminante $d(\alpha)$ der den Körper $K(\alpha)$ bestimmenden Gleichung

$$f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_\lambda) = 0 \tag{8}$$

durch p nicht teilbar ist. Denn in diesem Falle ist schon die Basis:

$$1, \ \alpha, \dots \alpha^{\lambda - 1} \tag{8a}$$

ein Fundamentalsystem modulo p für den Körper $K(\alpha)$, weil die Diskriminante:

$$d(\alpha) = |1, \ \alpha_i, \ \alpha_i^2, \dots \alpha_i^{\lambda-1}|^2 \qquad (i = 1, 2, \cdots \lambda) \tag{8b}$$

n. d. V. durch p nicht teilbar ist; also ist in dem Körper $K(\alpha)$ p selbst eine Primzahl, und jede p-adische Zahl desselben ist auf eine einzige Weise in der Form darstellbar:

$$\beta = \varepsilon^{(0)} + \varepsilon^{(1)}p + \cdots = \varepsilon^{(0)}, \varepsilon^{(1)}\varepsilon^{(2)} \dots .$$

Hier sind die Koeffizienten bestimmte modulo p reduzierte ganze algebraische Zahlen

$$\varepsilon = e_0 + e_1\alpha + \cdots + e_{\lambda-1}\alpha^{\lambda-1},$$

deren Koeffizienten e_i Zahlen der Reihe $0, 1, \dots p - 1$ sind.

Siebentes Kapitel.

Die Auflösung der ganzzahligen Gleichungen für den Bereich einer beliebigen Primzahl. Theorie der algebraischen Divisoren.

§ 1. Die p-adischen algebraischen Zahlen eines Körpers $K(\alpha)$ und die ganzen Funktionen mit p-adischen algebraischen Koeffizienten.

Durch die Ergebnisse des vorigen Kapitels sind wir dazu geführt worden, die p-adischen algebraischen Zahlen:

(1) $$\beta = \varepsilon^{(0)}, \varepsilon^{(1)} \varepsilon^{(2)} \ldots = \varepsilon^{(0)} + \varepsilon^{(1)}\pi + \varepsilon^{(2)}\pi^2 + \cdots$$

eines bestimmten Körpers $K(\alpha)$ in genau derselben Weise zu betrachten, wie wir früher die rationalen p-adischen Zahlen

(1a) $$B = e^{(0)}, e^{(1)} e^{(2)} \ldots = e^{(0)} + e^{(1)}p + e^{(2)}p^2 + \cdots$$

untersucht hatten. Das Hauptresultat war, daß die p-adischen algebraischen Zahlen wörtlich denselben Gesetzen gehorchen, wie die p-adischen rationalen Zahlen, nur tritt eben an die Stelle der rationalen Primzahl p die algebraische Primzahl π oder, was dasselbe ist, der algebraische Primdivisor $\mathfrak{p}$. Dann ergeben aber alle elementaren Rechenoperationen, bei ihrer Anwendung auf beliebige p-adische algebraische Zahlen wieder eindeutig bestimmte algebraische Zahlen als Resultate, welche nach genau denselben Regeln gefunden werden, wie in dem Gebiete der rationalen Zahlen.

Hieraus folgt, daß alle Sätze, welche wir für die rationalen p-adischen Zahlen bewiesen hatten, auch für die algebraischen p-adischen Zahlen eines bestimmten Körpers $K(\alpha)$ gültig bleiben, und daß dasselbe auch für die ganzen rationalen Funktionen:

(2) $$f(x) = A_0 x^n + A_1 x^{n-1} + \cdots + A_n$$

gilt, deren Koeffizienten jetzt nicht rationale, sondern algebraische p-adische Zahlen eines ein für allemale fest gewählten Körpers $K(\alpha)$ sind. Ich gebe daher hier nur jene Resultate an, und verweise auf die im dritten und vierten Kapitel gegebenen Beweise.

Ich nenne die gewöhnlichen ganzen algebraischen Zahlen

$$\beta^{(0)} = \varepsilon^{(0)};\ \beta^{(1)} = \varepsilon^{(0)}, \varepsilon^{(1)} = \varepsilon^{(0)} + \varepsilon^{(1)}\pi;\ \beta^{(2)} = \varepsilon^{(0)}, \varepsilon^{(1)}\,\varepsilon^{(2)} = \varepsilon^{(0)} + \varepsilon^{(1)}\pi + \varepsilon^{(2)}\pi^2; \cdots$$

den nullten, ersten, zweiten Näherungswert der ganzen p-adischen algebraischen Zahl β in (1) für den Bereich von $\mathfrak{p}$, und stelle die analoge Definition auch für die gebrochenen p-adischen algebraischen Zahlen auf. Diese präzisere Definition der Näherungswerte unterscheidet sich nur dadurch von der a. S. 127 gegebenen, daß dort die Entwicklung der p-adischen Zahlen noch nach Potenzen von $p \sim \pi^e$ erfolgen mußte; offenbar geht die Entwicklung von β nach Potenzen von π in die a. a. O. gegebene Entwicklung nach Potenzen von $p \sim \pi^e$ über, wenn man in (1) immer je e aufeinander folgende Glieder zu einem einzigen zusammenfasst.

Jede Funktion $f(x)$ in (2) kann man durch Division mit einer geeignet gewählten Zahl $\varepsilon\pi^\delta$ in der Form darstellen:

(3) $$f(x) = \varepsilon\pi^\delta f_0(x),$$

wo

(3a) $$f_0(x) = \pi^\varrho x^n + C_1 x^{n-1} + \cdots + C_n$$

eine primitive Funktion ist, d. h. eine Funktion, deren Koeffizienten $\pi^\varrho, C_1, \ldots C_n$ ganze algebraische Zahlen sind, von denen mindestens eine eine Einheit ist, und in welcher der Koeffizient der höchsten Potenz eine reine Potenz π^ϱ von π ist. Auch jetzt wollen wir die Funktion $f_0(x)$ primär nennen. Dann heißt π^δ der Zahlenteiler von $f(x)$. Da das Produkt von zwei primären Funktionen auch hier wieder primär ist, so besteht der Satz:

(I) Der Zahlenteiler eines Produktes zweier Funktionen ist dem Produkte der Zahlenteiler seiner Faktoren gleich.

Die ganze Funktion:

(4) $$f^{(k)}(x) = A_0^{(k)} x^n + A_1^{(k)} x^{n-1} + \cdots + A_n^{(k)},$$

welche aus $f(x)$ in (2) dadurch hervorgeht, daß dort jeder Koeffizient $A = \varepsilon^{(0)}, \varepsilon^{(1)}\,\varepsilon^{(2)} \ldots$ durch seinen k^{ten} Näherungswert $A^{(k)} = \varepsilon^{(0)}, \varepsilon^{(1)} \ldots \varepsilon^{(k)}$ ersetzt wird, nenne ich den k^{ten} Näherungswert jener Funktion. Dann bilden die Näherungswerte nullter, erster ... Ordnung von $f(x)$:

$$f^{(0)}(x),\quad f^{(1)}(x),\quad f^{(2)}(x), \ldots$$

eine Reihe wohldefinierter ganzer Funktionen mit gewöhnlichen algebraischen Koeffizienten. Ich nenne zwei Funktionen $f(x)$ und $\bar{f}(x)$ mit p-adischen algebraischen Koeffizienten kongruent modulo $\mathfrak{p}^{k+1}$,

wenn ihre k^{ten} Näherungswerte $f^{(k)}(x)$ und $\bar{f}^{(k)}(x)$ noch gleich sind, und ich bezeichne diese Beziehung folgendermaßen:

$$f(x) \equiv \bar{f}(x) \pmod{\mathfrak{p}^{k+1}}.$$

Dagegen sollen die beiden Funktionen gleich für den Bereich von $\mathfrak{p}$ heißen, wenn ihre Näherungswerte von genügend hoher Ordnung für jede noch so hohe Potenz von $\mathfrak{p}$ kongruent sind; dies ist dann und nur dann der Fall, wenn beide Funktionen gleiche Koeffizienten haben, also identisch sind.

Da das Euklidische Verfahren zur Bestimmung des größten gemeinsamen Teilers auf die Funktionen mit algebraischen Koeffizienten anwendbar bleibt, so gelten auch für diese die folgenden Sätze, welche nur Konsequenzen jener Tatsache sind:

> (II) Zwei Funktionen $f(x)$ und $g(x)$ mit algebraischen Koeffizienten besitzen stets einen größten gemeinsamen Teiler, welcher auf rationalem Wege, nämlich mit Hilfe des Euklididischen Verfahrens gefunden werden kann. Ist dieser Teiler eine Konstante, so heißen $f(x)$ und $g(x)$ teilerfremd. Dies letztere ist dann und nur dann der Fall, wenn ihre Resultante $R(f(x), g(x))$ von Null verschieden ist.

Eine Funktion $P(x)$ mit p-adischen algebraischen Koeffizienten des Bereiches $K(\alpha)$, welche sich nicht in solche Faktoren niedrigeren Grades zerlegen läßt, deren Koeffizienten demselben Bereiche $K(p, \alpha)$ angehören, heißt eine irreduktible oder Primfunktion. Auch hier beweist man genau ebenso, wie dies a. S. 66 flgde. geschehen ist, die Richtigkeit des Fundamentalsatzes:

> (III) Jede Funktion $F(x)$ läßt sich auf eine einzige Weise in Primfunktionen zerlegen, und es gibt ein endliches Verfahren, um diese Zerlegung mit jeder vorgegebenen Genauigkeit durchzuführen.

Die Frage, ob eine vorgelegte Funktion $F(x)$ dieses Bereiches in Faktoren zerfällt, und welches diese sind, wird durch den folgenden Satz beantwortet, der genau ebenso, wie das entsprechende Theorem a. S. 68—70 bewiesen wird:

> (IV) Ist die Diskriminante
>
> $$D(F(x)) = R(F(x),\ F'(x)) = \pi^{\delta} E \quad (\mathfrak{p})$$
>
> von $F(x)$ genau durch $\mathfrak{p}^{\delta}$ teilbar, so zerfällt die Funktion $F(x)$ dann und nur dann in Faktoren niedrigeren Grades, wenn ihr δ^{ter} Näherungswert $F^{(\delta)}(x)$ modulo $\mathfrak{p}^{\delta+1}$ zerfällt; die Frage, ob dies letztere der Fall ist oder nicht, kann durch eine endliche Anzahl von Versuchen gelöst werden (s. S. 67 oben).

Jeder Zerlegung von $F^{(\delta)}(x)$ modulo $\mathfrak{p}^{\delta+1}$:

$$F^{(\delta)}(x) \equiv \bar{f}(x)\,\bar{g}(x) \pmod{\mathfrak{p}^{\delta+1}}$$

in zwei Faktoren niedrigeren Grades $\bar{f}(x)$ und $\bar{g}(x)$ entspricht dann eine Zerlegung:

$$F(x) = f(x)\,g(x) \quad (\mathfrak{p})$$

der vorgelegten Funktion in zwei Faktoren der gleichen Grade, wie $\bar{f}$ bzw. $\bar{g}$ in der Weise, daß $\bar{f}(x)$ und $\bar{g}(x)$ bzw. die Näherungswerte von $f(x)$ und $g(x)$ sind. Diese Faktoren können sukzessive mit jeder vorgegebenen Genauigkeit berechnet werden.

Selbstverständlich bleiben alle Sätze über die Zerlegung einer Funktion innerhalb eines Körpers $K(\alpha)$ bestehen, wenn die zu untersuchende Funktion $F(x)$ rationale p-adische Koeffizienten hat, denn ihr Bereich bildet ja einen Teilbereich der algebraischen p-adischen Zahlen eines jeden Körpers $K(\alpha)$. Jede solche Funktion ist also innerhalb eines beliebigen algebraischen Körpers $K(p, \alpha)$ auf eine einzige Art in irreduktible Faktoren zerlegbar.

§ 2. Die Zerlegung der ganzen Funktionen in ihre p-adischen Linearfaktoren.

Das Gaußsche Fundamentaltheorem für den Bereich der p-adischen Zahlen.

Die im vorigen Paragraphen bewiesenen Sätze benutze ich nun zur Lösung der folgenden Fundamentalaufgabe:

Eine beliebig gegebene Funktion

$$f(x) = x^{\lambda} + a_1 x^{\lambda-1} + \cdots + a_{\lambda}$$

mit rationalen p-adischen Koeffizienten soll in einem geeignet gewählten algebraischen Körper in ein Produkt von λ Linearfaktoren $x - \xi_i$ so zerlegt werden, daß die Gleichung:

$$f(x) = (x - \xi_1)(x - \xi_2)\ldots(x - \xi_{\lambda}) \quad (p)$$

für ein variables x identisch erfüllt ist.

Ich werde diese Aufgabe vollständig lösen und zeigen, daß sie nur auf eine Weise gelöst werden kann. Ist das geschehen, so ist zugleich bewiesen, daß jede Gleichung $f(x) = 0$ für den Bereich einer beliebigen Primzahl p, stets genau so viele p-adische algebraische Wurzeln $(\xi_1, \xi_2, \ldots \xi_{\lambda})$ besitzt, als ihr Grad angibt, d. h. es ist damit das Gaußische Fundamentaltheorem in der Theorie der Gleichungen auch für den Bereich der p-adischen Zahlen bewiesen, wenn p irgend eine Primzahl bedeutet.

Ich brauche diese Aufgabe nur unter der Voraussetzung zu lösen, daß $f(x)$ für den Bereich der rationalen p-adischen Zahlen irreduktibel

ist, denn jede reduktible Funktion zerfällt ja eindeutig in irreduktible Faktoren; ist man also imstande, jede irreduktible Funktion in Linearfaktoren zu zerlegen, so gilt für die reduktiblen Funktionen dasselbe.

Zweitens braucht man nur einen der λ Linearfaktoren einer solchen Funktion zu bestimmen; ist dies nämlich geschehen, so ergeben sich, wie gleich gezeigt werden wird, die $\lambda - 1$ übrigen Faktoren aus diesem auf höchst einfache Weise.

Drittens wollen und können wir die Koeffizienten $a_1, \ldots a_\lambda$ der zu zerlegenden irreduktiblen Funktion $f(x)$ als ganze p-adische Zahlen voraussetzen; wären sie nämlich gebrochen und wäre p^ϱ ihr gemeinsamer Nenner, so führt die Substitution

$$x = \frac{y}{p^\varrho},$$

wie a. S. 119 unten bewiesen wurde, die irreduktible Funktion $f(x)$ in eine andere $g(y)$ über, in welcher der Koeffizient von y^λ ebenfalls gleich Eins ist und alle anderen ganze p-adische Zahlen sind, und aus der Zerlegung von $g(y)$ in Linearfaktoren ergibt sich ja diejenige von $f(x)$ ohne weiteres.

Ich stelle also jetzt die folgende Aufgabe:

Wie muß die algebraische Zahl α gewählt werden, damit die irreduktible ganzzahlige Funktion:

(1) $$f(x) = x^\lambda + a_1 x^{\lambda-1} + \cdots + a_\lambda$$

innerhalb des Körpers $K(\alpha)$ einen p-adischen Linearfaktor $x - \xi$ besitzt?

Es sei

(2) $$D(f) = p^\delta E$$

die Diskriminante von $f(x)$, und die ganze Funktion:

$$f^{(\delta)}(x) = x^\lambda + a_1^{(\delta)} x^{\lambda-1} + \cdots + a_\lambda^{(\delta)}$$

mit den nicht negativen ganzzahligen Koeffizienten $a_i^{(\delta)}$ sei der δ^{te} Näherungswert von $f(x)$; dann ist:

$$f(x) \equiv f^{(\delta)}(x), \quad D(f) \equiv D(f^{(\delta)}) \pmod{p^{\delta+1}},$$

und $f^{(\delta)}(x)$ ist ebenfalls modulo $p^{\delta+1}$, also auch für den Bereich der rationalen p-adischen Zahlen, irreduktibel, da ja sonst auch $f(x)$ wegen (IV) a. S. 155 zerlegbar sein müßte.

Soll nun $f(x)$ für den Bereich $K(\alpha)$ einen Linearfaktor besitzen, so muß nach dem soeben erwähnten Satze a. S. 155 α so gewählt werden, daß die ganzzahlige Funktion $f^{(\delta)}(x)$ modulo $p^{\delta+1}$ einen solchen Linearfaktor

erhält. Dies geschieht aber am einfachsten, wenn man für α eine der λ Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_\lambda$ der irreduktiblen Gleichung:

$$f^{(\delta)}(x) = 0,$$

etwa α_1, wählt, denn dann ist ja identisch

$$f^{(\delta)}(x) = (x - \alpha_1)\bar{f}^{(\delta)}(x),$$

also besteht natürlich auch modulo $p^{\delta+1}$ die Kongruenz:

$$f(x) \equiv (x - \alpha_1)\bar{f}^{(\delta)}(x) \pmod{p^{\delta+1}},$$

und aus ihr folgt nach dem bereits erwähnten Satze (IV) eine Zerlegung:

$$f(x) = (x - \xi_1)\bar{f}(x) \quad (p),$$

in welcher ξ_1 eine eindeutig bestimmte p-adische Zahl des durch α_1 konstituierten Körpers $K(\alpha_1)$ ist, deren Näherungswert eben jene Wurzel α_1 selbst ist.

Ist also α_1 eine der λ Wurzeln der irreduktiblen Gleichung

$$f^{(\delta)}(x) = 0,$$

ist π_1 die zugehörige Primzahl des Körpers $K(\alpha_1)$ und ist:

$$\alpha_1 = \varepsilon_1^{(0)}, \bar{\varepsilon}_1^{(1)}\bar{\varepsilon}_1^{(2)} \cdots = \varepsilon_1^{(0)} + \bar{\varepsilon}_1^{(1)}\pi_1 + \bar{\varepsilon}_1^{(2)}\pi_1^2 + \cdots$$

die Darstellung jener Wurzel α_1 als p-adische Zahl von $K(\alpha_1)$, dann gibt es eine eindeutig bestimmte p-adische Zahl desselben Körpers

$$\xi_1 = \varepsilon_1^{(0)}, \varepsilon_1^{(1)}\varepsilon_1^{(2)} \ldots,$$

welche dasselbe Anfangsglied besitzt wie α_1, aber in ihren späteren Ziffern von α_1 abweicht, und welche eine p-adische Wurzel der irreduktiblen Gleichung $f(x) = 0$ ist.

Hiermit ist die Aufgabe, eine Wurzel der irreduktiblen Gleichung (1) zu bestimmen, vollständig gelöst. Dasselbe Verfahren liefert aber auf einmal alle λ Wurzeln jener Gleichung und damit die vollständige Zerlegung ihrer linken Seite in Linearfaktoren. Ersetzt man nämlich die zuerst gewählte Wurzel α_1 von $f^{(\delta)}(x) = 0$ der Reihe nach durch ihren konjugierten $\alpha_2, \alpha_3, \ldots \alpha_\lambda$, so entsprechen diesen die λ konjugierten p-adischen algebraischen Zahlen

$$\xi_1, \xi_2, \ldots \xi_\lambda,$$

wo allgemein:

$$\xi_i = \varepsilon_i^{(0)} + \varepsilon_i^{(1)}\pi_i + \varepsilon_i^{(2)}\pi_i^2 + \cdots = \varepsilon_i^{(0)}, \varepsilon_i^{(1)}\varepsilon_i^{(2)} \cdots \quad (p)$$

ist, und von denen wir vorläufig nur wissen, daß die erste ξ_1 eine Wurzel der Gleichung $f(x) = 0$ ist. Sehr leicht zeigt man aber,

daß alle diese λ Zahlen voneinander verschieden sind und die Gleichung $f(x) = 0$ befriedigen. Bildet man nämlich die Funktion λ^{ten} Grades:

$$\bar{f}(x) = (x - \xi_1)(x - \xi_2) \cdots (x - \xi_\lambda) = x^\lambda + \bar{a}_1 x^{\lambda-1} + \cdots + \bar{a}_\lambda,$$

deren Wurzeln die Zahlen ξ_i sind, so ist diese nach dem a. S. 131 mitte bewiesenen Satze entweder irreduktibel oder die Potenz einer irreduktiblen Funktion mit rationalen p-adischen Koeffizienten, je nachdem alle ξ_i verschieden oder gewisse unter ihnen gleich sind. Andererseits haben die beiden Funktionen $f(x)$ und $\bar{f}(x)$ mindestens die eine Wurzel ξ_1 gemeinsam; da aber $f(x)$ nach der Voraussetzung irreduktibel ist, so muß $\bar{f}(x) = f(x)$ sein; also sind alle jene λ konjugierten algebraischen Zahlen ξ_i voneinander verschieden, und es besteht für ein variables x die identische Gleichung:

$$(3) \qquad f(x) = (x - \xi_1)(x - \xi_2) \cdots (x - \xi_\lambda) \quad (p).$$

Endlich erkennt man genau wie a. S. 52, daß die Gleichung $f(x) = 0$ keine weitere Wurzel ξ_0 haben kann, welche eine rationale oder algebraische p-adische Zahl ist. Setzt man nämlich in der Identität (3) $x = \xi_0$, so folgt aus der Gleichung:

$$(\xi_0 - \xi_1)(\xi_0 - \xi_2) \ldots (\xi_0 - \xi_\lambda) = 0 \quad (p),$$

daß mindestens einer dieser Faktoren gleich Null ist, d. h. daß seine Näherungswerte genügend hoher Ordnung durch jede noch so hohe Potenz von p teilbar sein müssen; und damit ist unsere Behauptung in ihrem vollen Umfange bewiesen.

Es ergibt sich so die folgende einfache Vorschrift für die vollständige Auflösung einer irreduktiblen Gleichung mit beliebigen rationalen p-adischen Koeffizienten.

Um die irreduktible Gleichung λ^{ten} Grades:

$$(4) \qquad f(x) = 0 \quad (p)$$

für den Bereich der p-adischen Zahlen vollständig aufzulösen, bilde man zuerst ihre Diskriminante. Ist δ die Ordnungszahl derselben, so löse man die Gleichung λ^{ten} Grades

$$(4\text{a}) \qquad f^{(\delta)}(x) = 0$$

auf, deren linke Seite der δ^{te} Näherungswert von $f(x)$ ist, welche also gewöhnliche positive ganzzahlige Koeffizienten besitzt. Ist dann:

$$(4\text{b}) \qquad f^{(\delta)}(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_\lambda)$$

die Zerlegung von $f^{(\delta)}(x)$ in die konjugierten Linearfaktoren, so entspricht ihr die Zerlegung:

(4c) $f(x) = (x - \xi_1)(x - \xi_2) \ldots (x - \xi_\lambda) \quad (p)$,

wo $\xi_1, \xi_2, \ldots \xi_\lambda$ eindeutig bestimmte konjugierte p-adische Zahlen der Körper $K(\alpha_1), \ldots K(\alpha_\lambda)$ sind, so daß also allgemein:

(4d) $\xi_i = \varepsilon_i^{(\varrho)} \pi_i^\varrho + \varepsilon_i^{(\varrho+1)} \pi_i^{\varrho+1} + \cdots \quad (p)$

ist, und daß α_i ein Näherungswert von ξ_i ist.

Jede im Bereich der rationalen p-adischen Zahlen irreduktible Gleichung λ^{ten} Grades besitzt also genau λ konjugierte p-adische Wurzeln, welche einen einzigen Zyklus bilden. Es ist auch klar, daß eine solche Gleichung λ^{ten} Grades (4) keine p-adische algebraische Zahl von niedrigerer als der λ^{ten} Ordnung als Wurzel haben kann. In der Tat, sei etwa

$$\eta_1 = \zeta_1^{(0)} + \zeta_1^{(1)} \varrho_1 + \zeta_1^{(2)} \varrho_1^2 + \cdots$$

eine Wurzel unserer Gleichung $f(x) = 0$, wo jetzt ϱ_1 der zu p gehörige Primfaktor ist, und sei diese Zahl nur von einer Ordnung $\mu < \lambda$. Sind dann

$$\eta_1, \eta_2, \ldots \eta_\mu$$

die μ zu η_1 konjugierten p-adischen Zahlen, und ist

$$h(x) = (x - \eta_1)(x - \eta_2) \cdots (x - \eta_\mu)$$

die Gleichung μ^{ten} Grades mit rationalen p-adischen Koeffizienten, der $\eta_1, \ldots \eta_\mu$ genügen, so hätten $h(x)$ und $f(x)$ wieder den Linearfaktor $(x - \eta_1)$ gemeinsam, also müßte die irreduktible Funktion $f(x)$ ein Teiler von $h(x)$ sein, was mit der oben gemachten Annahme $\mu < \lambda$ im Widerspruche steht.

Ich benutze dieses Resultat, um die allgemeinste in der Theorie der Gleichungen sich darbietende Aufgabe zu lösen. Es sei:

(5) $F(x) = A_0 x^n + A_1 x^{n-1} + \cdots + A_n = 0$

eine beliebige Gleichung n^{ten} Grades mit gewöhnlichen ganzzahligen positiven oder negativen Zahlkoeffizienten, und es sei p irgend eine reelle Primzahl. Wir stellen uns die Aufgabe, diese Gleichung im Bereich der p-adischen rationalen oder algebraischen Zahlen vollständig aufzulösen. Ich zerlege zu diesem Zwecke die Funktion $F(x)$ in ihre irreduktiblen Faktoren mit rationalen p-adischen Koeffizienten. Wir wollen der Einfachheit wegen annehmen, $F(x)$ zerfalle in drei solche Faktoren. Es sei:

(6) $F(x) = f(x)\, g(x)\, h(x) \quad (p)$

jene Zerlegung, und es mögen

$$\lambda,\ \mu,\ \nu$$

die Grade jener drei Faktoren sein, so daß $\lambda + \mu + \nu = n$ ist.

Dann besitzt die Gleichung:

$$f(x) = 0$$

innerhalb der λ konjugierten geeignet gewählten Körper

$$K(\alpha_1),\ K(\alpha_2), \ldots K(\alpha_\lambda)$$

die λ konjugierten Wurzeln $\xi_1, \xi_2, \ldots \xi_\lambda$, und es besteht die Identität:

$$f(x) = (x - \xi_1)(x - \xi_2) \ldots (x - \xi_\lambda) \quad (p). \tag{7}$$

Es mögen in derselben Weise:

$$\eta_1,\ \eta_2 \ldots \eta_\mu;\quad \zeta_1,\ \zeta_2, \ldots \zeta_\nu$$

die Wurzeln der beiden anderen irreduktiblen Gleichungen $g(x) = 0$ und $h(x) = 0$ im Gebiete der p-adischen Zahlen sein; auch diese bilden je einen Zyklus von μ bzw. ν konjugierten p-adischen algebraischen Zahlen, und es ist identisch:

$$g(x) = (x - \eta_1)(x - \eta_2) \ldots (x - \eta_\mu) \quad (p) \tag{7a}$$

$$h(x) = (x - \zeta_1)(x - \zeta_2) \ldots\ldots (x - \zeta_\nu). \quad (p) \tag{7b}$$

Setzt man diese Werte von $f(x)$, $g(x)$ und $h(x)$ in die Gleichung (6) ein, so ergibt sich die folgende Zerlegung von $F(x)$ in Linearfaktoren:

$$F(x) = A_0(x - \xi_1)\ldots(x - \xi_\lambda)\cdot(x - \eta_1)\ldots(x - \eta_\mu)\cdot(x - \zeta_1)\ldots(x - \zeta_\nu) \quad (p) \tag{8}$$

Es besteht also der Fundamentalsatz:

> Jede ganzzahlige Gleichung $F(x) = 0$ besitzt für den Bereich einer beliebigen Primzahl p genau so viele Wurzeln, als ihr Grad angibt, und diese ordnen sich in genau so viele Zyklen konjugierter p-adischer algebraischer Zahlen an, als die Anzahl der für den Bereich von p irreduktiblen Faktoren von $F(x)$ beträgt.

Die Wurzeln eines jeden Zyklus schreiten nach ganzen oder nach gebrochenen Potenzen der Primzahl p fort. Der letztere Fall kann aber nach dem a. S. 151 bewiesenen Satze nur dann eintreten, wenn die dem betreffenden irreduktiblen Faktor $f(x)$, $g(x)$ oder $h(x)$ entsprechende Körperdiskriminante durch p teilbar ist. Hieraus folgt leicht, daß überhaupt nur für eine endliche Anzahl von reellen Primzahlen gewisse Wurzelzyklen nach gebrochenen Potenzen derselben fortschreiten können. Bildet man nämlich die Diskriminante $D(F)$ der

vorgelegten Gleichung (2), so ist sie eine gewöhnliche positive oder negative ganze Zahl; sie enthält also nur eine endliche Anzahl:

$$q, r, \ldots s$$

von reellen Primzahlen als Teiler. Ist nun p eine nicht in $D(F)$ enthaltene Primzahl, so ergibt sich aus der Gleichung:

$$D(F) = D(f(x)\,g(x)\,h(x)) = \pm D(f)\,D(g)\,D(h)\,R^2(f,g)\,R^2(g,h)\,R^2(h,f),$$

daß keine einzige der Diskriminanten $D(f)$, $D(g)$ und $D(h)$ durch p teilbar ist. Nach dem soeben erwähnten Satze folgt also, daß die Wurzeln von allen drei hier auftretenden Zyklen nach ganzen Potenzen von p fortschreiten. Ist dagegen $D(F)$ durch p teilbar, so folgt aus der obigen Gleichung nur, daß gewisse unter den Diskriminanten

$$D(f),\ D(g),\ D(h)$$

p enthalten können, daß aber auch sehr wohl die Resultanten durch die links auftretende Potenz von p teilbar sein können. Aber selbst, wenn eine der drei Diskriminanten etwa $D(f(x))$ durch p teilbar ist, brauchen deshalb die λ Wurzeln des zugehörigen Zyklus noch nicht nach gebrochenen Potenzen von p fortzuschreiten, denn die zu $f(x) = 0$ gehörige Körperdiskriminante braucht ja nicht durch p teilbar zu sein, wenn die Gleichungsdiskriminante p enthält.

Wir wollen eine Primzahl p eine Verzweigungszahl für die Gleichung $F(x) = 0$ nennen, wenn mindestens ein Zyklus ihrer Wurzeln nach gebrochenen Potenzen von p fortschreitet. Dann kann das soeben erlangte Resultat in dem folgenden Satze ausgesprochen werden:

> Ist p eine beliebige Primzahl, so schreiten die n p-adischen Wurzeln der Gleichung n^{ten} Grades $F(x) = 0$ im allgemeinen nach ganzen Potenzen von p fort; nur für eine endliche Anzahl von Primzahlen, die sog. Verzweigungszahlen der Gleichung schreiten gewisse unter ihnen nach gebrochenen Potenzen von p fort; die Verzweigungszahlen sind gewisse unter den Diskriminantenteilern von $F(x)$.

§ 3. Die zu einer reellen Primzahl gehörigen algebraischen Primteiler.

Ich benutze jetzt die Resultate des vorigen Paragraphen, um die Zahlen eines Körpers $K(\alpha)$ in ihrer Beziehung zu einer Primzahl p unter der allgemeineren Voraussetzung zu untersuchen, daß die Grundgleichung für α:

(1) $$F(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

zwar für den Bereich $K(1)$ der gewöhnlichen rationalen Zahlen irreduktibel ist, dagegen für den Bereich der p-adischen rationalen Zahlen in irreduktible Faktoren niedrigeren Grades zerfällt. Und zwar will ich wieder annehmen, daß:

$$(2)\qquad F(x) = f(x)\,g(x)\,h(x) \quad (p)$$

diese Zerlegung von $F(x)$ ist. Ich hatte dann bewiesen, daß die Gleichung (1) genau n algebraische p-adische Wurzeln:

$$(3)\qquad \alpha_1, \alpha_2, \ldots \alpha_\lambda; \quad \alpha_{\lambda+1}, \alpha_{\lambda+2}, \ldots \alpha_{\lambda+\mu}; \quad \alpha_{\lambda+\mu+1}, \ldots \alpha_n$$

besitzt, deren Entwicklung nach ganzen oder gebrochenen Potenzen von p fortschreitet, und welche drei Zyklen konjugierter Reihen bilden, entsprechend den drei irreduktiblen Faktoren, in welche $F(x)$ in (2) zerfällt. Es mögen jene Reihen in (3) so bezeichnet sein, daß die λ ersten unter ihnen die Wurzeln der Gleichung $f(x) = 0$, die μ folgenden die Wurzeln von $g(x) = 0$ sind, so daß die ν letzten die sämtlichen Wurzeln von $h(x) = 0$ sind. Es sei wieder α irgend eine von diesen n Wurzeln.

Alle Sätze, welche über die n konjugierten Wurzeln, die eine irreduktible Gleichung ihrer Größe nach besitzt, und über die Eigenschaften aller rationalen Funktionen derselben im fünften Kapitel bewiesen wurden, gründen sich allein auf die Tatsache, daß für variable Werte von x die Identität

$$x^n + a_1 x^{n-1} + \cdots + a_n = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$$

besteht, und auf den Fundamentalsatz, daß ein Produkt dann und nur dann seiner Größe nach Null ist, wenn einer seiner Faktoren verschwindet. Da aber, wie wir gesehen haben, sowohl die obige Gleichung als auch jener Fundamentalsatz für die p-adischen algebraischen Zahlen erfüllt ist, so bleiben auch alle a. a. O. bewiesenen Folgerungen für den Bereich von p bestehen. Ich werde sie daher im folgenden benutzen und nun zeigen, in welcher Weise sie uns einen deutlichen Einblick in die Natur der algebraischen Zahlen gewähren.

Ich betrachte die Gesamtheit:

$$(4)\qquad \beta = \psi(\alpha)$$

aller rationalen Funktionen von α mit gewöhnlichen rationalen Koeffizienten, d. h. den durch α konstituierten algebraischen Zahlkörper $K(\alpha)$. Da die rationalen Zahlkoeffizienten von $\varphi(\alpha)$ für den Bereich von p gleich periodischen p-adischen Zahlen sind, so ist dieser Körper $K(\alpha)$ ein Teilbereich derjenigen p-adischen Zahlen

$$(4a)\qquad \gamma = \varphi(\alpha),$$

welche rationale Funktionen von α mit beliebigen, auch nicht periodischen rationalen p-adischen Koeffizienten sind. Diese Zahlen bilden den Bereich aller zum Körper $K(p, \alpha)$ gehörigen p-adischen algebraischen Zahlen und haben genau dieselben algebraischen Eigenschaften wie die Zahlen des Körpers $K(\alpha)$; daher sollen von vornherein diese p-adischen Zahlen genauer untersucht werden.

Ersetzt man in der Gleichung (4a) die Zahl α der Reihe nach durch $\alpha_1, \alpha_2, \ldots \alpha_n$, so erhält man entsprechend die n p-adischen algebraischen Zahlen:

(5) $$\gamma_1, \ldots \gamma_\lambda; \quad \gamma_{\lambda+1}, \ldots \gamma_{\lambda+\mu}; \quad \gamma_{\lambda+\mu+1}, \ldots \gamma_n,$$

wo allgemein:

(5a) $$\gamma_k = \varphi(\alpha_k)$$

ist. Nach dem a. S. 103 bei Nr. 4 bewiesenen Satze genügen diese ebenfalls einer Gleichung n^{ten} Grades:

(5b) $$G(x) = x^n + c_1 x^{n-1} + \cdots + c_n = (x - \gamma_1) \cdots (x - \gamma_n) = 0 \quad (p)$$

mit rationalen p-adischen Koeffizienten, und man zeigt jetzt leicht, daß $G(x)$ ebenso wie $F(x)$ selbst in drei p-adische Faktoren λ^{ten}, μ^{ten} und ν^{ten} Grades zerfällt, welche entweder selbst irreduktibel oder Potenzen irreduktibler Funktionen sind. Jede dieser rationalen Funktionen $\gamma_k = \varphi(\alpha_k)$ läßt sich nämlich genau wie α_k auf eindeutig bestimmte Weise in eine Reihe entwickeln, welche nach ganzen Potenzen von p oder von dem zu α_k gehörigen $\pi_k \sim p^{\frac{1}{e_k}}$ fortschreitet, und deren Koeffizienten eindeutig bestimmte modulo π_k reduzierte ganze algebraische Zahlen sind. Also sind auch die λ ersten Wurzeln $\gamma_1, \ldots \gamma_\lambda$ ebenso wie $\alpha_1, \ldots \alpha_\lambda$ konjugierte p-adische Zahlen, und das Produkt:

$$\bar{f}(x) = (x - \gamma_1) \cdots (x - \gamma_\lambda) = x^\lambda + d_1 x^{\lambda-1} + \cdots + d_\lambda$$

ist eine ganze Funktion mit rationalen p-adischen Koeffizienten, welche selbst irreduktibel oder die Potenz einer irreduktiblen Funktion ist, je nachdem alle konjugierten Zahlen $\gamma_1, \ldots \gamma_\lambda$ von einander verschieden sind oder nicht.

In derselben Weise sieht man, daß die μ folgenden Wurzeln

$$\gamma_{\lambda+1}, \ldots \gamma_{\lambda+\mu}$$

einen zweiten Zyklus konjugierter algebraischer p-adischer Zahlen bilden, und daß das gleiche für die ν letzten Wurzeln gilt. Hieraus ergibt sich auch für $G(x)$ die folgende Zerlegung in drei p-adische Faktoren des λ^{ten}, μ^{ten} und ν^{ten} Grades:

(6) $$G(x) = \bar{f}(x) \cdot \bar{g}(x) \cdot \bar{h}(x) \quad (p),$$

wo $\bar{g}(x)$ und $\bar{h}(x)$ aus den zum zweiten bzw. dritten Wurzelzyklus gehörigen Linearfaktoren bestehen.

Eine jede p-adische algebraische Zahl γ des Körpers $K(\alpha)$ genügt also nebst ihren n konjugierten einer Gleichung n^{ten} Grades mit rationalen p-adischen Koeffizienten, und deren linke Seite zerfällt in ebensoviele Faktoren mit rationalen Koeffizienten und vom gleichen Grade wie die entsprechende Grundgleichung. Jeder von diesen Faktoren ist entweder irreduktibel oder die Potenz einer irreduktiblen Funktion, und die n konjugierten Zahlen $\gamma_1, \gamma_2, \ldots \gamma_n$ zerfallen in genau ebensoviele Zyklen konjugierter Zahlen wie die Zahlen $\alpha_1, \ldots \alpha_n$, so daß jeder Wurzelzyklus die sämtlichen Wurzeln γ eines rationalen p-adischen Faktors bildet.

Ich betrachte nun die Wurzeln eines einzelnen, etwa des ersten Zyklus, d. h. die λ ersten Zahlen

(6a) $$\gamma_1, \gamma_2, \ldots \gamma_\lambda$$

der Reihe (5) etwas genauer. Sie alle stellen sich in der Form dar:

(6b) $$\gamma_i = \pi_i^\varrho \cdot \varepsilon_i = \varepsilon_i^{(\varrho)} \pi_i^\varrho + \varepsilon_i^{(\varrho+1)} \pi_i^{\varrho+1} + \cdots \qquad (i = 1, 2, \cdots \lambda),$$

wo π_i die zu dem Körper $K(\alpha_i)$ gehörige Primzahl, und ε_i eine Einheit dieses Körpers bezeichnet; alle λ konjugierten Zahlen (6b) sind dann von derselben Ordnungszahl.

Ich ordne nun diesem ersten, den λ Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_\lambda$ des ersten Faktors in (2):

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_\lambda) \quad (p)$$

entsprechenden Wurzelzyklus einen ersten Primteiler $\mathfrak{p}_f$ zu, und sage, die p-adische Zahl γ ist genau durch $\mathfrak{p}_f^\varrho$ teilbar, wenn die Wurzeln $\gamma_1, \gamma_2, \cdots \gamma_\lambda$ genau die Ordnungszahl ϱ besitzen, also genau durch π_i^ϱ teilbar sind.

In derselben Weise ordne ich dem zweiten und dem dritten Wurzelzyklus:

$$\alpha_{\lambda+1}, \ldots \alpha_{\lambda+\mu} \quad \text{und} \quad \alpha_{\lambda+\mu+1}, \ldots \alpha_n$$

oder dem zugehörigen zweiten und dritten Faktor in der Zerlegung (2):

$$g(x) = (x - \alpha_{\lambda+1}) \cdots (x - \alpha_{\lambda+\mu}) \quad \text{und} \quad h(x) = (x - \alpha_{\lambda+\mu+1}) \cdots (x - \alpha_n)$$

je einen Primfaktor

$$\mathfrak{p}_g \qquad \text{und} \qquad \mathfrak{p}_h$$

zu und sage, die algebraische Zahl γ ist genau durch

$$\mathfrak{p}_g^\sigma \qquad \text{bzw.} \qquad \mathfrak{p}_h^\tau$$

teilbar, wenn die μ Wurzeln $\gamma_{\lambda+1}, \ldots \gamma_{\lambda+\mu}$ des zweiten Zyklus die gemeinsame Ordnungszahl σ, bzw. wenn die ν Wurzeln $\gamma_{\lambda+\mu+1}, \ldots \gamma_n$ des letzten Zyklus die gemeinsame Ordnungszahl τ haben.

Dann entsprechen also der reellen Primzahl p drei voneinander verschiedene Primfaktoren $\mathfrak{p}_f, \mathfrak{p}_g, \mathfrak{p}_h$, die den drei irreduktiblen Faktoren $f(x)$, $g(x)$ und $h(x)$ oder den drei Wurzelzyklen (3) eindeutig zugeordnet sind, in welche die n Wurzeln der Grundgleichung, oder was dasselbe ist, in welche die n Wurzeln jeder Gleichung desselben Körpers zerfallen.

Jede Zahl γ des Körpers $K(\alpha)$ ist dann durch eine eindeutig bestimmte Potenz eines jeden unter diesen Primfaktoren genau teilbar, deren Exponent die Ordnungszahl der Wurzeln des diesem Divisor entsprechenden Zyklus ist.

Es sei nun β irgend eine andere Zahl unseres Körpers, welche genau durch $\mathfrak{p}_f^{\varrho'}$ teilbar ist, so daß also für die λ Zahlen $\beta_1, \ldots \beta_\lambda$ und $\gamma_1, \ldots \gamma_\lambda$ des ersten zu $\mathfrak{p}_f$ gehörigen Wurzelzyklus für β und γ die Darstellungen bestehen:

$$\beta_i = \pi_i^{\varrho'} \varepsilon_i', \qquad \gamma_i = \pi_i^{\varrho} \varepsilon_i. \qquad (i = 1, 2, \cdots \lambda)$$

Dann gelten für den ersten zu demselben Primteiler gehörigen Wurzelzyklus von $\beta\gamma$ und $\frac{\beta}{\gamma}$ bzw. die Gleichungen:

$$(\beta\gamma)_i = \beta_i \gamma_i = \pi_i^{\varrho+\varrho'} \varepsilon_i \varepsilon_i' = \pi_i^{\varrho+\varrho'} \bar{\varepsilon}_i,$$
$$\left(\frac{\gamma}{\beta}\right)_i = \frac{\gamma_i}{\beta_i} = \pi_i^{\varrho-\varrho'} \frac{\varepsilon_i}{\varepsilon_i'} = \pi_i^{\varrho-\varrho'} \bar{\bar{\varepsilon}}_i,$$

d. h. $\beta\gamma$ und $\frac{\gamma}{\beta}$ sind genau durch $\mathfrak{p}_f^{\varrho+\varrho'}$ bzw. $\mathfrak{p}_f^{\varrho-\varrho'}$ teilbar, und die entsprechenden Resultate gelten natürlich für jeden der drei zu p gehörigen Primteiler $\mathfrak{p}_f, \mathfrak{p}_g, \mathfrak{p}_h$.

Ist eine Zahl γ genau durch $\mathfrak{p}_f^{\varrho}$, durch $\mathfrak{p}_g^{\sigma}$ und durch $\mathfrak{p}_h^{\tau}$ teilbar, so wollen wir sagen, diese Zahl sei genau durch das Produkt

$$\mathfrak{p}_f^{\varrho} \mathfrak{p}_g^{\sigma} \mathfrak{p}_h^{\tau}$$

teilbar. Jede Zahl unseres Körpers ist durch ein solches eindeutig bestimmtes Potenzenprodukt genau teilbar, dessen Exponenten ϱ, σ und τ gleich den Ordnungszahlen der den Divisoren $\mathfrak{p}_f, \mathfrak{p}_g, \mathfrak{p}_h$ zugehörigen Wurzelzyklen sind.

Sind die beiden Zahlen γ und β bzw. genau durch die Produkte

$$\mathfrak{p}_f^{\varrho} \mathfrak{p}_g^{\sigma} \mathfrak{p}_h^{\tau} \quad \text{und} \quad \mathfrak{p}_f^{\varrho'} \mathfrak{p}_g^{\sigma'} \mathfrak{p}_h^{\tau'}$$

teilbar, so folgt aus den soeben durchgeführten Betrachtungen, daß ihr Produkt $\gamma\beta$ und ihr Quotient $\frac{\gamma}{\beta}$ bzw. genau durch:

$$\mathfrak{p}_f^{\varrho+\varrho'}\mathfrak{p}_g^{\sigma+\sigma'}\mathfrak{p}_h^{\tau+\tau'} \quad \text{und} \quad \mathfrak{p}_f^{\varrho-\varrho'}\mathfrak{p}_g^{\sigma-\sigma'}\mathfrak{p}_h^{\tau-\tau'}$$

oder, was dasselbe ist, durch:

$$(\mathfrak{p}_f^{\varrho}\mathfrak{p}_g^{\sigma}\mathfrak{p}_h^{\tau})\,(\mathfrak{p}_f^{\varrho'}\mathfrak{p}_g^{\sigma'}\mathfrak{p}_h^{\tau'}) \quad \text{und} \quad \frac{\mathfrak{p}_f^{\varrho}\mathfrak{p}_g^{\sigma}\mathfrak{p}_h^{\tau}}{\mathfrak{p}_f^{\varrho'}\mathfrak{p}_g^{\sigma'}\mathfrak{p}_h^{\tau'}}$$

teilbar ist.

Eine Zahl γ hieß algebraisch ganz für den Bereich von p, wenn die Gleichung n^{ten} Grades (5b), welcher sie genügt, lauter modulo p ganze Koeffizienten c_i hat. Aus der Zerlegung (6) für $G(x)$ folgt aber sofort, daß auch die drei Faktoren $\bar{f}(x)$, $\bar{g}(x)$ und $\bar{h}(x)$ dann und nur dann sämtlich modulo p ganze Koeffizienten haben, wenn für $G(x)$ dasselbe gilt. Zerfällt nämlich die primäre Funktion $G(x)$ (s. S. 64 (1)), in welcher der Koeffizient von x^n gleich 1 ist, in das Produkt $\bar{f}(x)\,\bar{g}(x)\,\bar{h}(x)$, so ist sie nach S. 64 (2) auch gleich dem Produkte $\bar{\bar{f}}(x)\,\bar{\bar{g}}(x)\,\bar{\bar{h}}(x)$ von drei primären Faktoren, welche sich von den vorigen höchstens um Zahlenfaktoren unterscheiden könnten; da sie aber ebenso wie diese als Koeffizienten der höchsten Potenz von x die Eins haben müssen, so sind sie mit jenen identisch, unsere Behauptung ist also bewiesen. Andererseits besitzt nach S. 140 Mitte z. B. der erste Faktor:

$$\bar{f}(x) = x^{\lambda} + a_1 x^{\lambda-1} + \cdots + a_{\lambda}$$

dann und nur dann modulo p gebrochene Koeffizienten, wenn die zu $\bar{f}(x)$ gehörigen Wurzeln $\gamma_1, \ldots \gamma_{\lambda}$ von negativer Ordnung sind, wenn also γ den diesem Zyklus zugehörigen Primteiler $\mathfrak{p}_f$ in negativer Potenz enthält und das Entsprechende gilt für die Primteiler $\mathfrak{p}_g$ und $\mathfrak{p}_h$. Hieraus folgt also der wichtige Satz:

> Eine algebraische Zahl γ ist dann und nur dann modulo p algebraisch ganz, wenn alle konjugierten Zahlen $\gamma_1, \ldots \gamma_n$ für den Bereich von p von nicht negativer Ordnung sind, oder was dasselbe ist, wenn γ in bezug auf jeden der zu p gehörigen Primteiler eine nicht negative Ordnungszahl besitzt.

Es sei γ eine algebraische Zahl unseres Körpers und es seien $\gamma_1, \gamma_2, \ldots \gamma_n$ die n konjugierten p-adischen Zahlen, welchen γ für den Bereich von p gleich ist. Dann folgt aus (5b):

$$(7) \qquad \gamma_1\gamma_2\cdots\gamma_n = (-1)^n c_n \quad (p).$$

Ich nannte diese rationale Zahl die volle Norm der algebraischen Zahl γ (vgl. S. 104 (5)) und bezeichnete sie durch

$$(7\text{a}) \qquad n(\gamma) = (-1)^n c_n.$$

Für den Bereich einer jeden Primzahl p ist $n(\gamma)$ also gleich dem Produkte aller konjugierten p-adischen Wurzeln. Zum Unterschiede wollen wir, wie a. a. O. schon erwähnt wurde, das entsprechende, aber nur über die Wurzeln des einen etwa zu $\mathfrak{p}_f$ gehörigen Zyklus erstreckte Produkt

(8) $$\gamma_1 \gamma_2, \cdots \gamma_\lambda = n_{\mathfrak{p}_f}(\gamma)$$

die in bezug auf $\mathfrak{p}_f$ gebildete Norm oder Partialnorm von γ nennen. Dann folgt aus der Definition der Partialnormen für $\mathfrak{p}_f$, $\mathfrak{p}_g$ und $\mathfrak{p}_h$ sofort die Gleichung:

(8a) $$n(\gamma) = n_{\mathfrak{p}_f}(\gamma) \cdot n_{\mathfrak{p}_g}(\gamma) \cdot n_{\mathfrak{p}_h}(\gamma) \quad (p).$$

Die volle Norm einer Zahl γ ist für den Bereich von p gleich dem Produkte ihrer Partialnormen in bezug auf alle zu p gehörigen Primfaktoren.

Ist nun γ genau durch das Produkt $\mathfrak{p}_f^\varrho \mathfrak{p}_g^\sigma \mathfrak{p}_h^\tau$ teilbar, und sind die Grade von $\mathfrak{p}_f$, $\mathfrak{p}_g$ und $\mathfrak{p}_h$ bzw. gleich f_0, g_0 und h_0, so ist in (8a) das Produkt rechts genau durch

(9) $$p^{\varrho f_0 + \sigma g_0 + \tau h_0}$$

teilbar. Hieraus folgt speziell, daß die Norm einer ganzen algebraischen Zahl γ dann und nur dann überhaupt durch die Primzahl p teilbar sein kann, wenn mindestens einer der drei Exponenten ϱ, σ oder τ positiv ist, wenn also γ mindestens durch einen der drei zu p gehörigen Primteiler $\mathfrak{p}_f$, $\mathfrak{p}_g$, $\mathfrak{p}_h$ in einer positiven Potenz teilbar ist. Ist nämlich γ modulo p algebraisch ganz, so kann keiner der drei Exponenten ϱ, σ und τ negativ sein, und sind sie alle drei Null, so ist nach (9) auch die volle Norm von γ genau durch p^0 teilbar.

§ 4. Der zu einer algebraischen Zahl gehörige Divisor.

Ist q eine beliebige reelle Primzahl, so besitzt die unseren Untersuchungen zu Grunde gelegte für den Bereich $K(1)$ der rationalen Zahlen irreduktible Gleichung:

(1) $$F(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0$$

für den Bereich von q genau n Wurzeln, welche sämtlich algebraische q-adische Zahlen sind. Diese Wurzeln ordnen sich in soviele Zyklen konjugierter q-adischer Zahlen, als die Anzahl h der irreduktiblen Faktoren mit rationalen q-adischen Koeffizienten beträgt, in welche $F(x)$ zerfällt.

Es sei nun:

(2) $$F(x) = k_1(x)\, k_2(x) \cdots k_h(x) \qquad (q)$$

jene Zerlegung, ferner:

(3) $k(x) = x^r + d_1 x^{r-1} + \cdots + d_r = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_r) \quad (q)$

einer dieser h irreduktiblen Faktoren, und

(3a) $$\beta_1, \beta_2, \cdots \beta_r$$

sei der zu ihm gehörige Wurzelzyklus; diese r konjugierten q-adischen Zahlen schreiten dann nach ganzen Potenzen von $\varkappa_1, \varkappa_2, \ldots \varkappa_r$ fort, wenn allgemein $\varkappa_i$ der zu $K(\beta_i)$ gehörige Primteiler von q ist. Jedem dieser h Faktoren $k(x)$, oder, was dasselbe ist, jedem dieser h Zyklen (3a) ordnen wir einen Primteiler zu. Es seien

(4) $$\mathfrak{q}_1, \mathfrak{q}_2, \cdots \mathfrak{q}_h$$

diese h Primteiler, und mit $\mathfrak{q}$ werde der zu $k(x)$ bzw. zu dem Zyklus $(\beta_1, \ldots \beta_r)$ gehörige Primteiler bezeichnet. Ist der zu $K(\beta_i)$ gehörige Primteiler $\varkappa_i \sim q^{\frac{1}{e}}$, so ist e, die Ordnung des Primteilers $\mathfrak{q}$, ein Teiler von r, und es werde wieder:

(5) $$r = ef$$

gesetzt.

Ist

(6) $$\gamma = \varphi(\beta)$$

irgend eine algebraische Zahl des Körpers $K(\beta)$ d. h. eine rationale Funktion von β mit gewöhnlichen rationalen Koeffizienten, so entspricht diesem Primteiler $\mathfrak{q}$ von q wieder ein Zyklus

(7) $$\gamma_1, \gamma_2, \cdots \gamma_r$$

konjugierter q-adischer Zahlen, welche mit den Zahlen des Zyklus (3a) durch die Gleichungen

$$\gamma_i = \varphi(\beta_i)$$

zusammenhängen. Jede dieser r Zahlen γ_i ist durch dieselbe eindeutig bestimmte Potenz $\mathfrak{q}^\varrho$ von $\mathfrak{q}$ teilbar, deren Exponent die Ordnungszahl des zu $\mathfrak{q}$ gehörigen Wurzelzyklus (7) angibt.

Man erkennt so, daß wir zu jeder reellen Primzahl q eine Anzahl h von Primteilern $\mathfrak{q}$ zugeordnet erhalten, welche jedesmal mit der Anzahl der irreduktiblen rationalen Faktoren der Grundgleichung für den Bereich von q übereinstimmt. Bei jeder algebraischen Zahl γ können wir angeben, wie oft ein jeder unter diesen Primteilern in γ enthalten ist; dieser Exponent ist nämlich gleich der gemeinsamen Ordnungszahl aller Wurzeln des zu $\mathfrak{q}$ gehörigen Wurzelzyklus.

Ist γ speziell eine **ganze** algebraische Zahl, d. h. besitzt die Gleichung n^{ten} Grades, der sie genügt, gar keine gebrochenen Koeffizienten, so ist sie auch in bezug auf jede reelle Primzahl q algebraisch ganz, d. h. sie ist durch keinen einzigen Primteiler $\mathfrak{q}$ in einer negativen Potenz genau teilbar. Ist dagegen γ nicht algebraisch ganz, so ist sie in bezug auf mindestens eine reelle Primzahl q nicht ganz, sie muß also mindestens einen der zu q gehörigen Primteiler $\mathfrak{q}$ in einer negativen Potenz enthalten. Wir erhalten somit die folgende charakteristische Eigenschaft aller ganzen algebraischen Zahlen, welche mit der entsprechenden Eigenschaft aller ganzen rationalen Zahlen vollkommen übereinstimmt.

> Eine algebraische Zahl γ ist dann und nur dann algebraisch ganz, wenn sie keinen einzigen Primteiler in einer negativen Potenz enthält, oder, was dasselbe ist, wenn ihre Entwicklungen für den Bereich einer jeden Primzahl q von nicht negativer Ordnung sind*).

Hieraus folgt leicht der Fundamentalsatz:

> Eine beliebige ganze oder gebrochene algebraische Zahl γ ist nur durch eine endliche Anzahl von Primfaktoren in einer positiven oder negativen Potenz teilbar.

Dies folgt zunächst für **ganze** algebraische Zahlen unmittelbar aus dem am Schluß des § 3 bewiesenen Satze: Nach diesem enthält nämlich die ganze Zahl γ dann und nur dann mindestens einen der zu q gehörigen Primteiler $\mathfrak{q}$, wenn ihre volle Norm $n(\gamma) = (-1)^n c_n$ mindestens einmal durch q teilbar ist. Da aber $n(\gamma)$ eine ganze rationale Zahl ist, also überhaupt nur eine endliche Anzahl reeller Primzahlen q als Teiler enthält, so ist γ wirklich nur durch eine endliche Anzahl von Primteilern $\mathfrak{q}$ teilbar, und durch Bildung der sämtlichen zu q gehörigen Wurzelzyklen kann man sich stets überzeugen, welche Primfaktoren $\mathfrak{q}$ in γ überhaupt auftreten und welche Potenz derselben in γ enthalten ist.

Es seien nun:

$$\mathfrak{p}^h, \mathfrak{q}^k, \mathfrak{r}^l, \ldots \mathfrak{t}^m$$

die sämtlichen voneinander verschiedenen Primdivisorenpotenzen, welche in einer ganzen algebraischen Zahl β genau enthalten sind — mögen diese nun zu lauter verschiedenen reellen Primzahlen gehören, oder

*) Dieses Theorem ist auch das vollständige Analogon zu dem bekannten Satze der Funktionentheorie, nach dem eine rationale oder eine algebraische Funktion einer Variablen dann und nur dann ganz ist, wenn ihre Entwicklung in der Umgebung einer jeden **endlichen** Stelle von nicht negativer Ordnung ist, wenn sie also im Endlichen keine Pole besitzt.

mögen gewisse unter ihnen nur verschiedene Primfaktoren derselben reellen Primzahl q sein, — so will ich diese Tatsache durch die Äquivalenz:

$$\beta \sim \mathfrak{p}^h \mathfrak{q}^k \mathfrak{r}^l \cdots \mathfrak{t}^m \tag{8}$$

ausdrücken; diese Äquivalenz bedeutet also, daß die zu $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots \mathfrak{t}$ gehörigen Wurzelzyklen von β bzw. die positiven Ordnungszahlen $h, k, l, \ldots m$ besitzen, während alle unendlich vielen übrigen Wurzelzyklen die Ordnungszahl Null haben, also Einheiten sind. Aus dieser Erklärung geht von selbst hervor, daß das auf der rechten Seite dieser Äquivalenz stehende Divisorenprodukt eindeutig bestimmt ist.

Dieselbe Darstellung im Sinne der Äquivalenz besteht natürlich auch für jede ganze rationale Zahl m, speziell für jede Primzahl q, und zwar ist:

$$q \sim \mathfrak{q}_1^{e_1} \mathfrak{q}_2^{e_2} \cdots \mathfrak{q}_h^{e_h}, \tag{8a}$$

wenn allgemein in dem zum Primdivisor $\mathfrak{q}_i$ gehörigen Wurzelzyklus die zugehörige Primzahl $x_i \sim q^{\frac{1}{e_i}}$ ist, denn in diesem Falle sind ja alle n zu q konjugierten Zahlen gleich q selbst, und es ist eben $q = \varepsilon_i x_i^{e_i}$.

Zur Abkürzung will ich im folgenden das auf der rechten Seite der Äquivalenz (8) stehende Divisorenprodukt durch einen Buchstaben $\mathfrak{d}_\beta$ bezeichnen und $\mathfrak{d}_\beta$ den zu β gehörigen Divisor nennen, so daß also

$$\beta \sim \mathfrak{d}_\beta = \mathfrak{p}^h \mathfrak{q}^k \mathfrak{r}^l \cdots \mathfrak{t}^m \tag{9}$$

ist. Dann gehört also zu jeder ganzen algebraischen Zahl β ein eindeutig bestimmter Divisor $\mathfrak{d}_\beta$. Ich nenne $\mathfrak{d}_\beta$ ferner einen ganzen Divisor, weil er keinen einzigen der in ihm auftretenden Primteiler in einer negativen Potenz enthält.

Jede ganze algebraische Zahl β ist also einem eindeutig bestimmten ganzen algebraischen Divisor äquivalent.

Ein ganzer Divisor $\mathfrak{d}_\beta$ bleibt im Sinne der Äquivalenz ungeändert, wenn man ihm irgend einen Primfaktor $\mathfrak{n}$ zur nullten Potenz erhoben hinzufügt; denn die Äquivalenz:

$$\beta \sim \mathfrak{n}^0 \mathfrak{p}^h \mathfrak{q}^k \cdots \mathfrak{t}^m \tag{9a}$$

besagt vollkommen dasselbe, wie die Äquivalenz (9), nur wird in der zweiten Äquivalenz noch explizite hervorgehoben, daß der zum Primdivisor $\mathfrak{n}$ gehörige Wurzelzyklus die Ordnungszahl Null besitzt, was aber auch aus (9) hervorgeht.

Es seien nun:

(10) $$\beta \sim \mathfrak{d}_\beta = \mathfrak{p}^h \mathfrak{q}^k \cdots \mathfrak{t}^m, \qquad \beta' \sim \mathfrak{d}_{\beta'} = \mathfrak{p}^{h'} \mathfrak{q}^{k'} \cdots \mathfrak{t}^{m'}$$

zwei beliebige ganze algebraische Zahlen, $\mathfrak{d}_\beta$ und $\mathfrak{d}_{\beta'}$ die zu ihnen gehörigen Divisoren, und wir nehmen diese der Einfachheit wegen als aus denselben Primteilern bestehend an, was ja auch erlaubt ist, da ja z. B. falls $\mathfrak{p}$ in $\mathfrak{d}_\beta$ nicht vorkommt, während dieser Primteiler in $\mathfrak{d}_{\beta'}$ enthalten ist, eben $h = 0$ anzunehmen ist. Dann gehört zu dem Produkte $\beta\beta'$ der Divisor:

(10a) $$\mathfrak{d}_{(\beta\beta')} = \mathfrak{p}^{h+h'} \mathfrak{q}^{k+k'} \ldots \mathfrak{t}^{m+m'},$$

d. h. das Produkt der den Faktoren entsprechenden Divisoren; denn besitzen z. B. die zu $\mathfrak{p}$ gehörigen beiden Wurzelzyklen von β und β' bzw. die Ordnungszahlen h und h', so besitzt nach dem a. S. 166 unten bewiesenen Satze der zu $\mathfrak{p}$ gehörige Zyklus von $\beta\beta'$ die Ordnungszahl $h + h'$ und das Entsprechende gilt für die übrigen Primteiler $\mathfrak{q}, \ldots \mathfrak{t}$.

Da ferner unter den obigen Voraussetzungen der zu $\mathfrak{p}$ gehörige Wurzelzyklus von $\frac{\beta}{\beta'}$ die Ordnungszahl $h - h'$ besitzt, usw., so entspricht dem Quotienten $\frac{\beta}{\beta'}$ der Divisor:

(10b) $$\mathfrak{d}_{\frac{\beta}{\beta'}} = \mathfrak{p}^{h-h'} \cdot \mathfrak{q}^{k-k'} \ldots \mathfrak{t}^{m-m'}.$$

Ist keine der Ordnungszahlen $h, k, \ldots m$ kleiner als die entsprechende $h', k', \ldots m'$, so gehört also auch zu dem Quotienten $\frac{\beta}{\beta'}$ ein ganzer Divisor; dieser Quotient ist eine ganze algebraische Zahl, d. h. β ist nach der a. S. 101 Mitte gegebenen Definition algebraisch durch β' teilbar. Ist dagegen auch nur einer der Exponenten von β kleiner als der entsprechende von β', so ist $\frac{\beta}{\beta'}$ eine gebrochene algebraische Zahl, und zu ihr gehört ein Divisor, welcher mindestens einen Primteiler in negativer Potenz enthält. Wir wollen auch solche Divisoren in den Kreis unserer Betrachtungen ziehen und sie als **gebrochene Divisoren** bezeichnen.

Da wir jede gebrochene algebraische Zahl β nach dem a. S. 100 (9b) bewiesenen Satze immer als den Quotienten:

$$\beta = \frac{\gamma}{b_0}$$

zweier ganzen algebraischen Zahlen darstellen können, von denen der Nenner sogar, was aber hier unwesentlich ist, eine ganze **rationale** Zahl ist, so entspricht auch jeder gebrochenen algebraischen Zahl β

eindeutig ein, und zwar ein gebrochener Divisor $\mathfrak{d}_\beta$, und wir erhalten ihn, wenn wir die zu γ und b_0 zugehörigen ganzen Divisoren $\mathfrak{d}_\gamma$ und $\mathfrak{d}_{b_0}$ bilden und nach (10b) ihren Quotienten:

$$\frac{\mathfrak{d}_\gamma}{\mathfrak{d}_{b_0}} = \mathfrak{d}_{\frac{\gamma}{b_0}} = \mathfrak{d}_\beta$$

aufsuchen. Da auch jetzt der zu der gebrochenen Zahl β gehörige Divisor die Ordnungszahlen der zu den einzelnen Primteilern gehörigen Wurzelzyklen von β bestimmt, so ist auch in diesem Falle der Divisor $\mathfrak{d}_\beta$ eindeutig bestimmt, und wir erhalten den folgenden Fundamentalsatz:

Jede algebraische Zahl ist einem eindeutig bestimmten algebraischen Divisor äquivalent, und dieser ist ganz oder gebrochen, jenachdem die zugehörige Zahl eine ganze oder eine gebrochene algebraische Zahl ist.

§ 5. Theorie der algebraischen Divisoren.

Im vorigen Paragraphen ist bewiesen worden, daß jede algebraische Zahl einem eindeutig bestimmten Divisor

$$\mathfrak{d} = \mathfrak{p}^h \mathfrak{q}^k \cdots \mathfrak{t}^m$$

zugeordnet ist. Im allgemeinen ist das Umgekehrte nicht richtig; wird der Divisor $\mathfrak{d}$ als ein Produkt von Primteilerpotenzen beliebig gegeben, so gibt es im allgemeinen keine Zahl β unseres Körpers, der $\mathfrak{d}$ äquivalent ist, für welche also die den Primteilern $\mathfrak{p}, \mathfrak{q}, \ldots \mathfrak{t}$ zugeordneten Wurzelzyklen die Ordnungszahlen $h, k, \ldots m$ haben, während alle übrigen Wurzeln Einheiten für die betreffenden Primteiler sind. Es wird eine Hauptaufgabe unserer späteren Untersuchungen sein, festzustellen, zu welchen Divisoren algebraische Zahlen gehören, zu welchen nicht.

Hierin liegt ein wesentlicher Unterschied zwischen den rationalen und den algebraischen Zahlen: Ist b eine beliebige rationale Zahl, so ist sie, abgesehen von einer Einheit, auf eine einzige Weise als Produkt von rationalen Primfaktoren, nämlich in der Form

$$b = e p^h q^k \cdots t^m \qquad (e = \pm 1)$$

darstellbar; und damit ist ausgedrückt, daß die der Zahl b gleiche rationale p-adische Zahl die Ordnungszahl h, die entsprechende q-adische Zahl die Ordnungszahl k hat usw., während b für den Bereich aller Primzahlen außer $p, q, \ldots t$ eine Einheit ist.

Umgekehrt gehört aber auch zu jedem beliebig gebildeten Divisorenprodukte

$$\mathfrak{d} = p^h q^k \cdots t^m,$$

abgesehen vom Vorzeichen stets eine rationale Zahl b, welche gerade diesen Divisor besitzt.

Ebenso nun, wie es in der Arithmetik der rationalen Zahlen vorteilhaft ist, jede Zahl als Produkt ihrer Primteiler darzustellen, also statt der Zahl b ihren Divisor $p^h q^k \cdots t^m$ zu betrachten, wollen wir hier auch bei allen Fragen der Teilbarkeit durch eine algebraische Zahl β lieber von dem dieser Zahl zugeordneten Divisor $\mathfrak{b}_\beta$ als von β selbst ausgehen. Dabei ist es nun in den meisten Fällen ganz gleichgültig, ob es eine Zahl β gibt, welcher der Divisor $\mathfrak{b}_\beta$ äquivalent ist, oder nicht. Wir wollen daher, um die Untersuchung der Teilbarkeit der algebraischen Zahlen durch gegebene Divisoren zu erleichtern, von vornherein diese Divisoren als selbständige Größen in unsere Betrachtungen aufnehmen, wie dies in der Arithmetik der rationalen Zahlen von selbst geschieht, weil hier alle jene rationalen Divisoren dem Körper der rationalen Zahlen angehören.

Die Elemente unserer Divisoren sind nach wie vor die sämtlichen zu den reellen Primzahlen gehörigen algebraischen Primteiler unseres Körpers $K(\alpha)$ und ihre positiven oder negativen Potenzen. Auch die nullten Potenzen $\mathfrak{p}^0$ eines beliebigen Divisors will ich mit hinzunehmen und hierunter, wie in der gewöhnlichen Arithmetik, die Zahl Eins verstehen.

Ich nenne dann jedes Produkt:

$$\mathfrak{b} = \mathfrak{p}^h \mathfrak{q}^k \cdots \mathfrak{t}^m$$

von beliebigen positiven oder negativen Potenzen beliebiger Primteiler einen algebraischen Divisor des Körpers $K(\alpha)$, indem ich jetzt ganz davon absehe, ob er einer Zahl dieses Körpers äquivalent ist, oder nicht. Ich werde zuerst die Grundregeln über das Rechnen mit diesen Divisoren angeben, und bemerke dabei gleich, daß sie wörtlich mit den Vorschriften der elementaren Arithmetik über das Rechnen mit den in ihre Primfaktoren zerlegten ganzen und gebrochenen Zahlen übereinstimmen. Wir werden dann sehen, wie sehr sich die Resultate und Methoden der ganzen Theorie durch die Einführung der algebraischen Divisoren vereinfachen.

Es seien:

(1) $$\mathfrak{b} = \mathfrak{p}^h \mathfrak{q}^k \cdots \mathfrak{r}^m, \qquad \mathfrak{b}' = \mathfrak{p}^{h'} \mathfrak{q}^{k'} \cdots \mathfrak{r}^{m'}$$

zwei beliebige aus denselben Primfaktoren $\mathfrak{p}, \mathfrak{q}, \ldots \mathfrak{r}$ bestehende Divisoren; dann definiere ich genau wie in der elementaren Arithmetik, ihr Produkt und ihren Quotienten durch die Gleichungen:

(1a) $$\mathfrak{b}\mathfrak{b}' = \mathfrak{p}^{h+h'} \mathfrak{q}^{k+k'} \cdots \mathfrak{r}^{m+m'}, \qquad \frac{\mathfrak{b}}{\mathfrak{b}'} = \mathfrak{p}^{h-h'} \mathfrak{q}^{k-k'} \cdots \mathfrak{r}^{m-m'}.$$

Ist einer der beiden Divisoren etwa $\mathfrak{d}' = \mathfrak{p}^0 \mathfrak{q}^0 \cdots \mathfrak{r}^0 = 1$, so will ich, wie in der elementaren Arithmetik, festsetzen, daß $\mathfrak{d} \cdot 1 = \mathfrak{d}$ ist, d. h. daß ein Divisor ungeändert bleibt, wenn man ihn mit der nullten Potenz einer oder mehrerer Primteiler multipliziert. Somit gilt unsere Definition des Produktes und des Quotienten zweier Divisoren auch dann, wenn sie nicht aus denselben Primteilern bestehen, da man ja wie vorher (s. S. 172 oben) z. B. zu $\mathfrak{d}$ die Potenz $\mathfrak{p}^0$ hinzufügen kann, falls der Primteiler $\mathfrak{p}$ nicht in $\mathfrak{d}$ vorkommen sollte.

Ein Divisor:

$$\mathfrak{g} = \mathfrak{p}^g \mathfrak{q}^{g'} \cdots \mathfrak{t}^{g^{(\mu)}}$$

heißt ganz, wenn kein einziger seiner Exponenten $g, g', \ldots g^{(\mu)}$ negativ ist; ist dagegen auch nur einer dieser Exponenten negativ, so heißt er ein gebrochener Divisor.

Jeder gebrochene Divisor $\mathfrak{d}$ kann als der Quotient zweier ganzen Divisoren, nämlich in der Form:

$$\mathfrak{d} = \frac{\mathfrak{p}^g \mathfrak{q}^{g'} \cdots \mathfrak{t}^{g^{(\mu)}}}{\mathfrak{p}^{\bar{h}} \mathfrak{q}^{\bar{h}'} \cdots \mathfrak{r}^{\bar{h}^{(\nu)}}} = \frac{\mathfrak{z}}{\mathfrak{n}} \tag{2}$$

geschrieben werden, wo der Zähler $\mathfrak{z}$ alle Primfaktoren mit positiven, der Nenner $\mathfrak{n}$ alle Primfaktoren mit negativen Exponenten enthält.

Einen solchen Bruch $\mathfrak{d} = \frac{\mathfrak{z}}{\mathfrak{n}}$ können wir uns in seiner reduzierten Form geschrieben denken, in welcher Zähler und Nenner keinen gemeinsamen Teiler, d. h. keinen gemeinsamen Primfaktor $\mathfrak{p}$ zugleich enthalten; aber $\mathfrak{d}$ bleibt auch ungeändert, wenn man den Bruch $\frac{\mathfrak{z}}{\mathfrak{n}}$ mit einem beliebigen ganzen Divisor $\mathfrak{g}$ „erweitert"; es ist nämlich identisch:

$$\mathfrak{d} = \frac{\mathfrak{z}}{\mathfrak{n}} = \frac{\mathfrak{z}\mathfrak{g}}{\mathfrak{n}\mathfrak{g}}, \tag{2a}$$

weil die Multiplikation mit dem Quotienten $\frac{\mathfrak{g}}{\mathfrak{g}} = 1$ den Divisor $\mathfrak{d}$ ungeändert läßt.

Ein Divisor $\mathfrak{d}$ heißt durch einen anderen $\mathfrak{d}'$ teilbar, wenn der Quotient:

$$\frac{\mathfrak{d}}{\mathfrak{d}'} = \mathfrak{g} \tag{3}$$

ein ganzer Divisor ist, wenn also $\mathfrak{d}$ jeden Primfaktor $\mathfrak{p}$ ebenso oft oder öfter enthält als $\mathfrak{d}'$.

Sind $\mathfrak{d}$ und $\mathfrak{d}'$ zwei beliebige ganze oder auch gebrochene Divisoren, so nennen wir den Divisor:

$$\mathfrak{D} = (\mathfrak{d}, \mathfrak{d}')$$

ihren **größten gemeinsamen Teiler**, welcher jeden einzelnen Primteiler $\mathfrak{p}$ so oft enthält, als er mindestens in $\mathfrak{d}$ und $\mathfrak{d}'$ auftritt. Ist $\mathfrak{D}$ so bestimmt, so sind $\mathfrak{d}$ und $\mathfrak{d}'$ offenbar beide durch $\mathfrak{D}$ teilbar, d. h. es ist:

$$\text{(3a)} \qquad \mathfrak{d} = \mathfrak{D}\mathfrak{g}, \qquad \mathfrak{d}' = \mathfrak{D}\mathfrak{g}',$$

wo $\mathfrak{g}$ und $\mathfrak{g}'$ ganze Divisoren sind, welche keinen einzigen Primteiler $\mathfrak{p}$ gemeinsam haben, und die daher **teilerfremde** oder **relativ prime** ganze Divisoren genannt werden können. Ist z. B.:

$$\mathfrak{d} = \frac{\mathfrak{p}^7 \mathfrak{r}^{13} \mathfrak{t}^2}{\mathfrak{q}^3 \mathfrak{z}^9}, \qquad \mathfrak{d}' = \frac{\mathfrak{p}^3 \mathfrak{q}^4}{\mathfrak{r}^9 \mathfrak{v}^5},$$

so findet man $\mathfrak{D}$, indem man jeden der sechs in $\mathfrak{d}$ und $\mathfrak{d}'$ auftretenden Primteiler, mit dem kleineren von den beiden zugehörigen Exponenten versehen, zu einem Produkt vereinigt. So erhält man:

$$\mathfrak{D} = \frac{\mathfrak{p}^3}{\mathfrak{q}^3 \mathfrak{r}^9 \mathfrak{z}^9 \mathfrak{v}^5},$$

ferner ist:

$$\mathfrak{d} = \mathfrak{D}(\mathfrak{p}^4 \mathfrak{r}^{22} \mathfrak{v}^5 \mathfrak{t}^2), \qquad \mathfrak{d}' = \mathfrak{D}(\mathfrak{q}^7 \mathfrak{z}^9),$$

und man erkennt, daß die beiden ganzen Divisoren

$$\mathfrak{g} = \mathfrak{p}^4 \mathfrak{r}^{22} \mathfrak{v}^5 \mathfrak{t}^2, \qquad \mathfrak{g}' = \mathfrak{q}^7 \mathfrak{z}^9$$

in der Tat teilerfremd sind.

In gleicher Weise kann man auch den größten gemeinsamen Teiler:

$$\text{(4)} \qquad \mathfrak{D} = (\mathfrak{d}_1, \mathfrak{d}_2, \cdots \mathfrak{d}_\nu)$$

mehrerer Divisoren definieren und in jedem einzelnen Falle direkt hinschreiben. Sind die ν Divisoren $\mathfrak{d}_i$ sämtlich ganz, also alle Exponenten ihrer Primteiler $\mathfrak{p}, \mathfrak{q}, \ldots$ positiv oder Null, so ist auch $\mathfrak{D}$ ein ganzer Divisor, da er jeden einzelnen Primteiler so oft enthält, als er mindestens in allen Divisoren $\mathfrak{d}_i$ auftritt; sind dagegen nicht alle Divisoren $\mathfrak{d}_i$ ganz, enthält also auch nur einer einen Primteiler etwa $\mathfrak{p}$ in der negativen Potenz $\mathfrak{p}^{-h}$, so besitzt $\mathfrak{D}$ ebenfalls einen Faktor $\mathfrak{p}^{-\bar{h}}$, dessen Exponent $\bar{h} \geqq h$ ist, d. h. auch $\mathfrak{D}$ ist ein gebrochener Divisor. Also gilt der Satz:

Der größte gemeinsame Teiler beliebig vieler Divisoren ist dann und nur dann ganz, wenn das Gleiche für alle jene Divisoren gilt.

Jedem Primteiler $\mathfrak{p}$ entspricht eindeutig eine reelle Primzahl p, nämlich diejenige, welche durch $\mathfrak{p}$ teilbar ist. Ist f der Grad von $\mathfrak{p}$, so setzen wir:

$$\text{(5)} \qquad n(\mathfrak{p}) = p^f.$$

Sind $\pi_1, \pi_2, \ldots \pi_\lambda$ konjugierte Primzahlen der λ zu $\mathfrak{p}$ gehörigen Körper, so ist p^f gleich der in dem Produkte $\pi_1 \pi_2 \ldots \pi_\lambda$ enthaltenen Potenz von p. Ich will p^f die zu dem Primteiler $\mathfrak{p}$ gehörige Primzahlpotenz nennen.

Ich erweitere nun den Begriff der Norm auf zusammengesetzte Divisoren, und zwar durch die Festsetzung, daß für zwei beliebige Divisoren $\mathfrak{d}$ und $\mathfrak{d}'$, mögen dieselben ganz oder gebrochen sein, stets:

$$(5a) \qquad n(\mathfrak{d} \cdot \mathfrak{d}') = n(\mathfrak{d})\, n(\mathfrak{d}')$$

sein soll. Hierdurch in Verbindung mit der Definitionsgleichung (5) für die Norm eines Primteilers ist die Norm eines beliebigen Divisors vollständig erklärt, denn zunächst ist für eine Primteilerpotenz:

$$(5b) \qquad n(\mathfrak{p}^h) = (n(\mathfrak{p}))^h = p^{fh},$$

und für einen beliebig zusammengesetzten Divisor:

$$(5c) \qquad n(\mathfrak{p}^h \mathfrak{q}^k \cdots \mathfrak{r}^l) = p^{fh} q^{gk} \cdots r^{jl},$$

wenn $p^f, q^g, \cdots r^j$ die zu den Primteilern $\mathfrak{p}, \mathfrak{q}, \cdots \mathfrak{r}$ gehörigen Primzahlpotenzen bedeuten. So ergibt sich also die folgende allgemeine Definition:

> Zu jedem algebraischen Divisor $\mathfrak{d}$ gehört eine eindeutig bestimmte rationale Zahl $n(\mathfrak{d})$, welche dadurch aus $\mathfrak{d}$ hervorgeht, daß man jeden in $\mathfrak{d}$ auftretenden Primteiler $\mathfrak{p}, \mathfrak{q}, \ldots$ durch die zugehörige Primzahlpotenz $p^f, q^g, \ldots$ ersetzt.

Hieraus folgt, daß die Norm eines ganzen Divisors eine ganze rationale Zahl sein muß; dagegen kann auch die Norm eines gebrochenen Divisors $\mathfrak{d} = \frac{\mathfrak{z}}{\mathfrak{n}}$ ganz sein, denn im Zähler und im Nenner von $\mathfrak{d}$ können ja Primteiler $\mathfrak{p}_1$ und $\mathfrak{p}_2$ auftreten, welche zu derselben reellen Primzahl p gehören, und die zugehörigen Normen p^{f_1} und p^{f_2} können sich ganz oder zum Teile fortheben.

Ich wende diese Resultate jetzt auf die Zahlen β des Körpers $K(\alpha)$ und die speziellen ihnen zugehörigen Divisoren $\mathfrak{d}_\beta$ an. Aus dem a. S. 171 flgde. gefundenen Resultate ergibt sich sofort der wichtige Satz:

> Jeder Zahl β entspricht eindeutig ein ihr äquivalenter algebraischer Divisor. Sind
>
> $$\beta \sim \mathfrak{d}_\beta, \qquad \beta' \sim \mathfrak{d}_{\beta'}$$
>
> zwei beliebige Zahlen, so ist
>
> $$\beta\beta' \sim \mathfrak{d}_\beta \mathfrak{d}_{\beta'}, \qquad \frac{\beta}{\beta'} \sim \frac{\mathfrak{d}_\beta}{\mathfrak{d}_{\beta'}}.$$

In der Tat sind ja die a. S. 172 (10a) und (10b) gefundenen zu $\beta\beta'$ und $\frac{\beta}{\beta'}$ äquivalenten Divisoren bzw. gleich $\mathfrak{d}_\beta \mathfrak{d}_{\beta'}$ und $\frac{\mathfrak{d}_\beta}{\mathfrak{d}_{\beta'}}$.

Eine Zahl ist dann und nur dann algebraisch ganz, wenn der ihr äquivalente Divisor ebenfalls ganz ist. Jede gebrochene Zahl β ist äquivalent einem gebrochenen Divisor:

$$\beta \sim \frac{\mathfrak{z}_\beta}{\mathfrak{n}_\beta},$$

dessen Zähler und Nenner ganze teilerfremde Divisoren sind.

Zwei beliebige ganze oder gebrochene algebraische Zahlen β und β' haben stets einen größten gemeinsamen Teiler

$$\mathfrak{d}_{(\beta,\beta')} = (\beta, \beta') = (\mathfrak{d}_\beta, \mathfrak{d}_{\beta'});$$

derselbe ist gleich dem größten gemeinsamen Teiler der beiden zugehörigen Divisoren. Dieser größte gemeinsame Teiler ist dann und nur dann ein ganzer Divisor, wenn β und β' beide algebraisch ganz sind.

Ist nämlich auch nur eine dieser Zahlen gebrochen, so enthält ihr Divisor ja mindestens einen Primteiler in negativer Potenz, und dasselbe gilt dann, wie a. S. 176 unten gezeigt wurde, auch für den größten gemeinsamen Teiler.

Im allgemeinen werden wir uns nur mit dem größten gemeinsamen Teiler von zwei oder mehreren g a n z e n algebraischen Zahlen beschäftigen. Zwei g a n z e Zahlen heißen r e l a t i v p r i m oder t e i l e r f r e m d, wenn die zugehörigen Divisoren teilerfremd sind, oder, was dasselbe ist, wenn sie keinen einzigen Primteiler gemeinsam haben.

Von zwei Zahlen β und γ heißt die erste durch die zweite teilbar, wenn der Quotient $\frac{\beta}{\gamma}$ algebraisch ganz ist, wenn also $\mathfrak{d}_\beta$ durch $\mathfrak{d}_\gamma$ teilbar ist. Ist auch umgekehrt γ durch β teilbar, so heißen sie äquivalent; dies ist dann und nur dann der Fall, wenn ihre Divisoren $\mathfrak{d}_\beta$ und $\mathfrak{d}_\gamma$ gleich sind. Sind β und γ äquivalent, so ist $\beta = \gamma\varepsilon$, und ε ist eine algebraische Einheit. Wir nannten eine algebraische Zahl ε eine Einheit, wenn sowohl sie selbst als ihr reziproker Wert $\frac{1}{\varepsilon}$ algebraisch ganz ist. Dies ist dann und nur dann der Fall, wenn der ihr zugehörige Divisor $\mathfrak{d}_\varepsilon$ und der zu $\frac{1}{\varepsilon}$ gehörige $\frac{1}{\mathfrak{d}_\varepsilon}$ ganz, wenn also $\mathfrak{d}_\varepsilon \sim 1$ ist.

Eine Zahl ε ist also stets und nur dann eine Einheit, wenn der zugehörige Divisor $\mathfrak{d}_\varepsilon \sim 1$ ist.

Es sei nun β eine beliebige algebraische Zahl, und

$$n(\beta) = (-1)^n b_n$$

ihre Norm, also b_n das konstante Glied der zu β gehörigen Gleichung $G(y) = 0$. Ist dann $\mathfrak{d}_\beta$ der β äquivalente Divisor, und $n(\mathfrak{d}_\beta)$ die nach der soeben gegebenen Regel gebildete Norm desselben, so folgt aus dem a. S. 168 geführten Beweise sofort, daß

$$n(\beta) = \pm n(\mathfrak{d}_\beta)$$

ist, daß also jene beiden Normen abgesehen vom Vorzeichen gleich sind. In der Tat, gehören zu irgend einer reellen Primzahl p etwa drei Primteiler $\mathfrak{p}_f$, $\mathfrak{p}_g$, $\mathfrak{p}_h$, und ist β genau durch das Produkt

$$\mathfrak{p}_f^\varrho \mathfrak{p}_g^\sigma \mathfrak{p}_h^\tau$$

teilbar, so ist nach dem a. a. O. gegebenen Beweise $n(\beta) = \beta_1 \beta_2 \cdots \beta_n$ genau durch:

$$p^{f_0 \varrho + g_0 \sigma + h_0 \tau}$$

teilbar, wenn p^{f_0}, p^{g_0}, p^{h_0} die zu den Divisoren $\mathfrak{p}_f$, $\mathfrak{p}_g$, $\mathfrak{p}_h$ gehörigen Primzahlpotenzen sind. Genau dieselbe Potenz von p enthält aber nach dem a. S. 177 Mitte gegebenen Bildungsgesetze (5c) auch $n(\mathfrak{d}_\beta)$, und da dasselbe für jede einzelne reelle Primzahl gilt, so ist unsere Behauptung vollständig bewiesen. Hieraus folgt noch speziell der a. S. 102 bereits anderweitig bewiesene Satz, daß die Norm einer algebraischen Einheit stets gleich ± 1 ist, weil ja der zu einer Einheit gehörige Divisor gleich Eins ist.

Achtes Kapitel.

Untersuchung der algebraischen Zahlen eines Körpers für den Bereich eines Primdivisors.

§ 1. Die äquivalenten Fundamentalsysteme und die äquivalenten Primzahlen für den Bereich von $\mathfrak{p}$.

Die allgemeinste Aufgabe, auf die sich alle Teilbarkeitsfragen zurückführen lassen, kann folgendermaßen gefaßt werden:

> Es soll ein vollständiges System aller algebraischen Zahlen eines Körpers $K(\alpha)$ gefunden werden, welche durch einen gegebenen Divisor $\mathfrak{d}$ teilbar sind.

Wir werden leicht zeigen, daß diese allgemeine Aufgabe auf den einfachen Fall zurückgeführt werden kann, daß $\mathfrak{d} = \mathfrak{p}^a$ die Potenz eines Primteilers ist. Diese spezielle Frage läßt sich nun höchst einfach lösen, wenn wir das Verhalten der Zahlen des Körpers für den Bereich dieses Primteilers überhaupt genauer kennen gelernt haben.

Ich gehe daher zunächst zu dieser Untersuchung über, und werde jetzt zeigen, daß die algebraischen p-adischen Zahlen für den Bereich eines Primteilers $\mathfrak{p}$ genau dieselben einfachen Eigenschaften haben, wie sie den rationalen p-adischen Zahlen in bezug auf die reelle Primzahl p zukommen.

Es sei also $\mathfrak{p}$ ein beliebiger Primteiler des Körpers $K(\alpha)$, welcher zu der reellen Primzahl p gehört, e sei die Ordnung, f der Grad dieses Divisors, so daß also

(1) $$n(\mathfrak{p}) = p^f$$

ist; endlich werde wieder

(2) $$ef = \lambda$$

gesetzt. Ich untersuche nun alle rationalen Funktionen:

(3) $$\beta = \varphi(\alpha)$$

der algebraischen Zahl n^{ter} Ordnung α mit beliebigen rationalen p-adischen Koeffizienten. In diesem größeren Bereiche bilden die Zahlen des Körpers $K(\alpha)$, d. h. die Funktionen von α mit gewöhnlichen ganzzahligen oder rational gebrochenen Koeffizienten einen Teilbereich; denn diese sind ja für den Bereich von p allen und nur den Funktionen $\beta = \varphi(\alpha)$ gleich, deren Koeffizienten lauter periodische p-adische Zahlen sind. Alle hier abzuleitenden Resultate gelten somit auch für die Zahlen von $K(\alpha)$ und auf sie werden sie dann angewendet werden.

Zu dem Divisor $\mathfrak{p}$ gehören nun $ef = \lambda$ konjugierte p-adische algebraische Zahlen

$$\beta_1, \beta_2, \ldots \beta_\lambda, \tag{4}$$

die einen Zyklus konjugierter Wurzeln derjenigen Gleichung n^{ten} Grades

$$G(y) = 0 \qquad (\mathfrak{p})$$

bilden, welcher die Zahl β für den Bereich von $\mathfrak{p}$ genügt. Es sei β eine von diesen λ algebraischen Zahlen (4), dann läßt sie sich folgendermaßen darstellen:

$$\beta = \varepsilon^{(0)} + \varepsilon^{(1)}\pi + \varepsilon^{(2)}\pi^2 + \cdots \quad (\mathfrak{p}), \tag{5}$$

wo die Koeffizienten eindeutig bestimmte Zahlen eines vollständigen Restsystems

$$\overset{(0)}{\varepsilon}, \overset{(1)}{\varepsilon}, \overset{(2)}{\varepsilon}, \ldots \overset{(\sigma-1)}{\varepsilon} \qquad (\sigma = p^f) \tag{6}$$

für den Primdivisor $\mathfrak{p}$ sind, und wo

$$\pi \sim p^{\frac{1}{e}} \tag{6a}$$

irgend eine Primzahl für den Bereich von $\mathfrak{p}$, d. h. eine Zahl ist, welche einmal und nur einmal durch den Primteiler $\mathfrak{p}$ teilbar ist.

Bei der Auswahl der σ Zahlen des vollständigen Restsystems (6) hat man nun eine sehr große Freiheit: Ist nämlich

$$\overset{(0)}{\eta}, \overset{(1)}{\eta}, \overset{(2)}{\eta}, \ldots \overset{(\sigma-1)}{\eta} \tag{6b}$$

irgend ein anderes vollständiges Restsystem für den Körper $K(\alpha)$ in bezug auf den Primdivisor $\mathfrak{p}$, dessen Elemente der Einfachheit wegen gleich so geordnet sein mögen, daß allgemein:

$$\overset{(i)}{\eta} \equiv \overset{(i)}{\varepsilon} \quad (\text{mod. } \mathfrak{p}) \qquad (i = 0, 1, \cdots \sigma - 1) \tag{7}$$

ist, so kann man jede Zahl β auch nach Potenzen von π, aber so entwickeln, daß bei der Darstellung:

$$\beta = \eta^{(0)} + \eta^{(1)}\pi + \eta^{(2)}\pi^2 + \cdots \quad (\mathfrak{p}) \tag{8}$$

von β die Koeffizienten $\eta^{(i)}$ nun eindeutig bestimmte Zahlen des Systems (6b) sind. Da nämlich jede ganze Zahl unseres Bereiches modulo $\mathfrak{p}$ betrachtet einer und nur einer Zahl der Reihe (6b) kongruent ist, so kann man ja, falls β algebraisch ganz ist, auch jetzt, wie a. S. 145 (3b), ein System von Gleichungen aufstellen:

$$\begin{aligned} \beta \; &= \eta^{(0)} + \pi \beta^{(1)}, \\ \beta^{(1)} &= \eta^{(1)} + \pi \beta^{(2)}, \\ &\vdots \end{aligned}$$

aus dem sich genau ebenso wie a. a. O. die Entwicklung (8) von β ergibt; und das Entsprechende gilt, wenn β in bezug auf $\mathfrak{p}$ von negativer Ordnung sein sollte.

Von dieser Freiheit in der Wahl der Restsysteme werde ich nun Gebrauch machen, um die Entwicklungen der algebraischen Zahlen für den Bereich von p möglichst einfach zu gestalten. Auch schon bei den rationalen p-adischen Zahlen

$$A = a_0 + a_1 p + a_2 p^2 + \cdots = a_0, a_1 a_2 \cdots \quad (p),$$

wo die Ziffern a_i Zahlen des vollständigen Restsystems

(9) $$0,\ 1,\ 2,\ \cdots p-1$$

für den Modul p sind, braucht dieses keineswegs immer das passendste System zu sein. Für viele Untersuchungen, speziell für diejenigen, welche sich auf die Theorie der quadratischen Reste und auf das Reziprozitätsgesetz beziehen, ist es z. B. einfacher, statt des obigen Systems das folgende:

(9a) $$-\frac{p-1}{2},\ \cdots -1,\ 0,\ +1,\ \cdots +\frac{p-1}{2}$$

zu wählen. In vielen Fällen erweist sich das System

(9b) $$0,\ 1,\ \omega,\ \omega^2,\ \ldots\ \omega^{p-2}$$

als noch viel geeigneter, wo ω eine primitive $(p-1)^{\text{te}}$ Einheitswurzel, d. h. eine primitive Wurzel der Gleichung

$$x^{p-1} - 1 = 0 \quad (p)$$

ist, welche ja eine bestimmte rationale p-adische Zahl ist; denn wir hatten im § 6 des vierten Kapitels bewiesen, daß auch diese Zahlen, modulo p betrachtet, den Zahlen (9), abgesehen von ihrer Reihenfolge, kongruent sind, also ebenfalls ein vollständiges Restsystem modulo p bilden. So ergibt sich also der Satz:

Jede rationale p-adische Zahl läßt sich auf eine einzige Weise in der Form

$$A = \omega^{(r)} p^r + \omega^{(r+1)} p^{r+1} + \cdots$$

darstellen, in welcher die Koeffizienten $\omega^{(k)}$ entweder $(p-1)^{\text{te}}$ Einheitswurzeln oder Null sind, also eindeutig bestimmte Zahlen aus der Reihe (9b) der sämtlichen Wurzeln der Gleichung:

$$(10) \qquad x^p - x = 0 \quad (p).$$

Alle Sätze der elementaren Zahlentheorie sind einfache Folgerungen gerade aus dieser Darstellung der Zahlen für den Bereich von p. Ich werde zeigen, daß eine unmittelbare Verallgemeinerung dieser Entwicklung für die Darstellung der algebraischen Zahlen für den Bereich eines beliebigen Primteilers $\mathfrak{p}$ besteht und zu einer wunderbar einfachen Herleitung der arithmetischen Eigenschaften aller algebraischen Zahlen führt.

Neben der zweckmäßigen Wahl des Restsystemes (6) für den Modul $\mathfrak{p}$ kann man die Darstellung der Zahlen β auch durch die Auswahl der Entwicklungszahl π in (6a) ganz wesentlich vereinfachen. In der Tat ist jene Zahl π nur durch die Forderung beschränkt, daß sie für den Bereich von $\mathfrak{p}$ eine Primzahl sein muß; jede andere Zahl

$$(11) \qquad \pi' = \varepsilon^{(1)} \pi + \varepsilon^{(2)} \pi^2 + \cdots,$$

in welcher nur $\varepsilon^{(1)}$ eine Einheit sein muß, kann also an Stelle von π als Entwicklungszahl gewählt werden. Diese Tatsache werde ich im folgenden benutzen, um für π die einfachste unter allen diesen äquivalenten Primzahlen (11) aufzusuchen.

§ 2. Die Fundamentalsysteme modulo $\mathfrak{p}$.

Ich will zunächst zeigen, wie man in dem Bereiche aller p-adischen algebraischen Zahlen des Körpers $K(p, \alpha)$ ein ebenso einfaches vollständiges Restsystem modulo $\mathfrak{p}$ finden kann, wie es für den Bereich der rationalen p-adischen Zahlen und die Primzahl p das System $(0, 1, \omega, \omega^2, \ldots \omega^{p-2})$ der $(p-1)^{\text{ten}}$ Einheitswurzeln ist.

Zu diesem Zwecke leite ich zunächst eine allen Einheiten modulo $\mathfrak{p}$ von $K(p, \alpha)$ gemeinsame Eigenschaft her, welche eine direkte Verallgemeinerung des für die ganzen rationalen Zahlen geltenden s. g. kleinen Fermatschen Satzes ist. Es sei wieder

$$(1) \qquad \overset{(1)}{\varepsilon}, \overset{(2)}{\varepsilon}, \ldots \overset{(\sigma-1)}{\varepsilon} \qquad (\sigma = p^f)$$

ein vollständiges System modulo $\mathfrak{p}$ inkongruenter Einheiten von $K(p, \alpha)$, und ε irgend eine Einheit desselben Bereiches. Dann bilden die $\sigma - 1$ Produkte

$$(1\,\mathrm{a})\qquad \varepsilon\overset{(1)}{\varepsilon},\ \varepsilon\overset{(2)}{\varepsilon},\ \ldots\ \varepsilon\overset{(\sigma-1)}{\varepsilon}$$

ebenfalls ein vollständiges System modulo $\mathfrak{p}$ inkongruenter Einheiten; denn einmal sind diese $\sigma - 1$ Zahlen sämtlich Einheiten, und zweitens können nicht zwei unter ihnen kongruent sein, da aus einer Kongruenz

$$\varepsilon\overset{(i)}{\varepsilon} \equiv \varepsilon\overset{(k)}{\varepsilon} \pmod{\mathfrak{p}}, \qquad \overset{(i)}{\varepsilon} \equiv \overset{(k)}{\varepsilon} \pmod{\mathfrak{p}}$$

folgen würde, was unserer Voraussetzung über das System (1) widerstreitet. Da somit die Einheiten der beiden Reihen (1) und (1a), abgesehen von ihrer Reihenfolge, modulo $\mathfrak{p}$ kongruent sind, so muß das Produkt der Einheiten (1a) dem der Einheiten (1) kongruent sein, und aus der Kongruenz:

$$\varepsilon^{\sigma-1}\left(\overset{(1)}{\varepsilon}\,\overset{(2)}{\varepsilon}\ldots\overset{(\sigma-1)}{\varepsilon}\right) \equiv \left(\overset{(1)}{\varepsilon}\,\overset{(2)}{\varepsilon}\ldots\overset{(\sigma-1)}{\varepsilon}\right) \pmod{\mathfrak{p}}$$

ergibt sich durch Division mit $\left(\overset{(1)}{\varepsilon}\ldots\overset{(\sigma-1)}{\varepsilon}\right)$ die Richtigkeit des folgenden Satzes:

Jede Einheit modulo $\mathfrak{p}$ des Bereiches $K(p, \alpha)$ genügt der Kongruenz:

$$(2)\qquad \varepsilon^{p^f-1} \equiv 1 \pmod{\mathfrak{p}}.$$

Die Kongruenz:

$$(2\,\mathrm{a})\qquad x^{p^f-1} - 1 \equiv 0 \pmod{\mathfrak{p}}$$

besitzt also innerhalb des Bereiches $K(p, \alpha)$ genau so viele modulo $\mathfrak{p}$ inkongruente Wurzeln als ihr Grad angibt, nämlich alle $\sigma - 1 = p^f - 1$ modulo $\mathfrak{p}$ inkongruenten Einheiten (1) dieses Bereiches.

Ebenso, wie die Kongruenz (2a) besitzt auch die Kongruenz:

$$(2\,\mathrm{b})\qquad H_f(x) = x^{p^f} - x \equiv 0 \pmod{\mathfrak{p}},$$

deren linke Seite aus der von (2a) durch Multiplikation mit x hervorgeht, genau p^f inkongruente Lösungen, nämlich alle Zahlen

$$\overset{(0)}{\varepsilon},\ \overset{(1)}{\varepsilon},\ \ldots\ \overset{(\sigma-1)}{\varepsilon}$$

eines vollständigen Restsystemes modulo $\mathfrak{p}$; denn zu den Einheiten (1) ist nur noch die eine Zahl $\overset{(0)}{\varepsilon} \equiv 0 \pmod{\mathfrak{p}}$ hinzugekommen, welche ja der Kongruenz (2b) offenbar auch genügt. Da somit:

$$H_f(x) = H_f\left(\overset{(i)}{\varepsilon}\right) + \left(x - \overset{(i)}{\varepsilon}\right)\bar{H}_i(x) \equiv \left(x - \overset{(i)}{\varepsilon}\right)\bar{H}_i(x) \pmod{\mathfrak{p}}$$

ist, also $H_f(x)$ modulo $\mathfrak{p}$ betrachtet jeden der σ inkongruenten Linearfaktoren $\left(x - \overset{(i)}{\varepsilon}\right)$ enthält, so besteht der Satz:

Ist $\left(\overset{(0)}{\varepsilon}, \overset{(1)}{\varepsilon}, \overset{(2)}{\varepsilon}, \ldots \overset{(\sigma-1)}{\varepsilon}\right)$ irgend ein vollständiges Restsystem für den Körper $K(\alpha)$ und den Primteiler $\mathfrak{p}$, so besteht modulo $\mathfrak{p}$ für ein variables x die Zerlegung:

$$(2\text{c}) \qquad H_f(x) = x^{p^f} - x \equiv \left(x - \overset{(0)}{\varepsilon}\right)\left(x - \overset{(1)}{\varepsilon}\right) \cdots \left(x - \overset{(\sigma-1)}{\varepsilon}\right) \pmod{\mathfrak{p}}.$$

Aus diesem Satze ziehe ich jetzt eine Folgerung, welche viel wichtiger ist, als dieses Theorem selbst, und welche uns sofort das einfachste vollständige Restsystem modulo $\mathfrak{p}$ ergibt. Es gilt nämlich der folgende Satz:

Die Gleichung:

$$(3) \qquad H_f(x) = x^{p^f} - x = 0 \qquad (\mathfrak{p})$$

besitzt innerhalb der p-adischen algebraischen Zahlen von $K(\alpha)$ stets p^f voneinander verschiedene Wurzeln

$$(3\text{a}) \qquad \overset{(0)}{\eta}, \overset{(1)}{\eta}, \ldots \overset{(\sigma-1)}{\eta} \qquad (\sigma = p^f),$$

d. h. es ist identisch:

$$x^{p^f} - x = \left(x - \overset{(0)}{\eta}\right)\left(x - \overset{(1)}{\eta}\right) \cdots \left(x - \overset{(\sigma-1)}{\eta}\right) \qquad (\mathfrak{p});$$

diese Zahlen $\left(\overset{(0)}{\eta}, \overset{(1)}{\eta}, \ldots \overset{(\sigma-1)}{\eta}\right)$ bilden modulo $\mathfrak{p}$ betrachtet ebenfalls ein und zwar das einfachste vollständige Restsystem für den Körper $K(p, \alpha)$.

Um diesen Satz zu beweisen, zeige ich, daß zu jeder Zahl $\varepsilon = \overset{(i)}{\varepsilon}$ des vollständigen Restsystemes $\left(\overset{(0)}{\varepsilon}, \ldots \overset{(\sigma-1)}{\varepsilon}\right)$ eine ihr modulo $\mathfrak{p}$ kongruente $\eta = \overset{(i)}{\eta}$ d. h. eine Zahl

$$(4) \qquad \eta = \varepsilon + \varepsilon'\pi + \varepsilon''\pi^2 + \cdots$$

unseres Bereiches gefunden werden kann, welche der algebraischen Gleichung (3) genügt. In der Tat ist ε eine Wurzel der Kongruenz

$$H_f(x) \equiv 0 \pmod{\mathfrak{p}},$$

d. h. es ist $H_f(\varepsilon)$ mindestens durch $\mathfrak{p}$ teilbar; andererseits ist aber

$$H_f'(x) = p^f x^{p^f - 1} - 1 \equiv -1 \pmod{\mathfrak{p}},$$

also $H_f'(\varepsilon)$ ist sicher nicht durch $\mathfrak{p}$ teilbar. Somit ist der Quotient

$$\frac{H_f(\varepsilon)}{(H_f'(\varepsilon))^2}$$

mindestens von der ersten, jedenfalls von positiver Ordnung modulo $\mathfrak{p}$. Nach dem a. S. 71 (3) bewiesenen Satze kann man also wirklich innerhalb des Bereiches $K(p, \alpha)$ eine Zahl $\eta = \overset{(i)}{\eta}$ von der Form (4) finden, welche der Gleichung (3) genügt, und die zu $\varepsilon = \overset{(i)}{\varepsilon}$ modulo $\mathfrak{p}$ kongruent ist; und da dasselbe für jede der p^f Zahlen $\overset{(i)}{\varepsilon}$ gilt, so ist unsere Behauptung vollständig bewiesen.

Da

$$x^{p^f} - x = x(x^{p^f-1} - 1)$$

ist, so ist eine der Wurzeln $\overset{(i)}{\eta}$ von (3) gleich Null; wir wollen $\overset{(0)}{\eta} = 0$ annehmen. Dann sind die übrigen Zahlen $\left(\overset{(1)}{\eta}, \overset{(2)}{\eta}, \ldots \overset{(\sigma-1)}{\eta}\right)$ unseres vollständigen Restsystemes modulo $\mathfrak{p}$ die sämtlichen Wurzeln der reinen Gleichung:

$$x^{p^f-1} = 1 \qquad (\mathfrak{p}),$$

sie sind also alle $(p^f - 1)^{\text{te}}$ Wurzeln der Einheit für den Bereich von p.

Dieses Resultat scheint mir merkwürdig genug, um einen Augenblick bei ihm zu verweilen. Es zeigt nämlich, daß, wie auch der zu untersuchende Körper $K(\alpha)$ beschaffen sein mag, und welche reelle Primzahl p auch gewählt werde, die Koeffizienten $\eta^{(i)}$ aller p-adischen algebraischen Zahlen dieses Körpers

(5) $$\beta = \eta^{(r)}\pi^r + \eta^{(r+1)}\pi^{r+1} + \cdots \quad (\mathfrak{p}),$$

falls sie nicht Null sind, immer als Einheitswurzeln gewählt werden können, und daß ihr Grad $(p^f - 1)$ allein von dem Grade f des betreffenden Primteilers $\mathfrak{p}$ abhängt. Nur diese Einheitswurzeln sind also als neue Irrationalitäten dem Bereiche der p-adischen Zahlen zu adjungieren, um die Koeffizienten aller überhaupt existierenden algebraischen p-adischen Zahlen zu erhalten.*) Aus diesem Grunde sollen im nächsten Paragraphen die sehr einfachen Eigenschaften dieser neu einzuführenden algebraischen Zahlen η genauer untersucht werden.

§ 3. Die Eigenschaften der Wurzeln der allgemeinen Gleichung $x^{p^f-1} = 1$.

Es sei η eine der $(p^f - 1)$ Wurzeln der Gleichung:

(1) $$x^{\sigma-1} = x^{p^f-1} = 1 \qquad (p).$$

*) Besitzt dieselbe Primzahl p für einen anderen Körper $K(\gamma)$ einen Primteiler desselben Grades f, so besitzt die Gleichung (3) innerhalb des Bereiches $K(p, \gamma)$ ebenfalls $\sigma = p^f - 1$ Wurzeln $\left(\overset{(0)}{\zeta}, \overset{(1)}{\zeta}, \cdots \overset{(\sigma-1)}{\zeta}\right)$, welche den Zahlen (3a) abgesehen von der Reihenfolge für den Bereich von p gleich sind.

Dann folgt genau ebenso, wie a. S. 81 (3), daß alle Potenzen $(1, \eta, \eta^2, \ldots)$ jene Gleichung ebenfalls befriedigen, weil allgemein

$$(\eta^k)^{\sigma-1} = (\eta^{\sigma-1})^k = 1 \quad (p)$$

ist; und da die Gleichung (1) überhaupt nur $(\sigma - 1)$ Wurzeln hat, so ergibt sich genau wie a. a. O., daß es einen kleinsten Exponenten d gibt, für welchen

(1a) $$\eta^d = 1 \quad (p)$$

ist, und daß die $d - 1$ ersten Potenzen von η

(1b) $$1, \eta, \eta^2, \ldots \eta^{d-1}$$

voneinander verschiedene Wurzeln der Gleichung (1) sind. Ich sage wieder, daß die Wurzel η zu diesem Exponenten d **gehört**, wenn η^d die kleinste Potenz von η ist, welche gleich Eins ist. Dann erkennt man, daß eine Potenz η^k von η dann und nur dann gleich Eins ist, wenn k ein Multiplum von d ist. Da aber wegen (1) für jede Wurzel η $\eta^{\sigma-1} = 1$ ist, so muß der Exponent $\sigma - 1 = p^f - 1$ durch jeden Exponenten d teilbar sein, zu dem eine Wurzel η gehört. Es ergibt sich also der Satz:

Jede der $(p^f - 1)$ Einheiten $\overset{(1)}{\eta}, \overset{(2)}{\eta}, \ldots \overset{(\sigma-1)}{\eta}$ gehört zu einem Exponenten d, welcher ein Teiler von $(p^f - 1)$ oder gleich $(p^f - 1)$ selbst ist.

Es sei nun für jeden der Divisoren d von $(p^f - 1)$ $\psi(d)$ die Anzahl der Wurzeln η, welche gerade zu diesem Exponenten d gehören, so daß also $\psi(d) = 0$ zu setzen wäre, wenn etwa zu dem Exponenten d keine einzige Wurzel η gehören sollte. Da jede dieser $(p^f - 1)$ Wurzeln zu einem und nur einem Teiler d von $(p^f - 1)$ gehören muß, so ergibt sich ohne weiteres, daß die über alle Teiler d von $p^f - 1$ erstreckte Summe:

(2) $$\sum_{(d)} \psi(d) = p^f - 1$$

ist.

Es sei nun d irgend ein Teiler von $(p^f - 1)$, und ich nehme an, es existiere wenigstens eine Wurzel η, welche gerade zu diesem Exponenten d gehört. Dann ist $\eta^d = 1$, d. h. η ist eine Wurzel der Gleichung:

(3) $$x^d - 1 = 0 \quad (p);$$

aber auch die d Potenzen

(3a) $$1, \eta, \eta^2, \ldots \eta^{d-1}$$

welche nach (1b) alle von einander verschieden sind, genügen derselben Gleichung, weil ja für jede Potenz η^k offenbar $(\eta^k)^d = (\eta^d)^k = 1$ ist.

Da die Gleichung d^{ten} Grades (3) nicht mehr als d Wurzeln haben kann, so gibt es auch keine andere Wurzel von (1), deren d^{te} Potenz gleich Eins ist. Man findet also die Anzahl $\psi(d)$ aller zum Exponenten d gehörigen $(p^f-1)^{\text{ten}}$ Einheitswurzeln, wenn man die Anzahl der Potenzen η^k in (3a) aufsucht, welche zum Exponenten d gehören, für welche also keine niedrigere Potenz

$$(\eta^k)^{d'} = \eta^{kd'} = 1 \quad (p) \qquad\qquad (d' < d)$$

ist. Soll aber für einen bestimmten Exponenten k $\eta^{kd'} = 1$ sein, so muß der Exponent kd' durch d teilbar sein. Da nun die kleinste Zahl d', für welche

$$kd' \equiv 0 \pmod{d}$$

ist, bekanntlich gleich

$$\frac{d}{(k,\,d)}$$

ist, wo (k, d) den größten gemeinsamen Teiler von k und d bedeutet, so erkennt man, daß alle und nur die $\varphi(d)$ Potenzen η^k von η zum Exponenten d selbst gehören, für welche $(k, d) = 1$, d. h. der Exponent k zu d teilerfremd ist. Existiert also wenigstens eine zum Exponenten d gehörige Einheitswurzel η, so gibt es im ganzen genau $\varphi(d)$ Einheitswurzeln, welche dieselbe Eigenschaft haben. Die Anzahl $\psi(d)$ aller zu einem gegebenen Teiler d von (p^f-1) als Exponenten gehörigen Einheitswurzeln ist mithin stets entweder gleich $\varphi(d)$ oder gleich Null.

Diese zweite Möglichkeit kann nun für keinen Divisor eintreten; denn da für die arithmetische Funktion $\varphi(d)$ bekanntlich dieselbe Gleichung

$$\sum_{(d)} \varphi(d) = p^f - 1$$

besteht, wie für die Zahlen $\psi(d)$, so kann keine einzige Zahl $\psi(d) = 0$ sein, da sonst mindestens eine andere Zahl $\psi(d') > \varphi(d')$ sein müßte. Es ergibt sich also der wichtige Satz:

> Es gibt genau $\varphi(d)$ Einheitswurzeln, welche zu einem gegebenen Teiler d von (p^f-1) als Exponenten gehören; da $\varphi(d)$ stets mindestens gleich Eins ist, so gibt es also zu jedem Teiler d mindestens eine zum Exponenten d gehörige Einheitswurzel.

Von besonderer Wichtigkeit sind die s. g. primitiven $(p^f-1)^{\text{ten}}$ Wurzeln der Einheit, nämlich diejenigen, welche zu dem Exponenten (p^f-1) selbst gehören; ich will diese primitiven Einheitswurzeln auch primitive Einheiten modulo $\mathfrak{p}$ des Bereiches $K(p, \alpha)$ nennen. Welchen Wert auch f habe, immer existieren solche primitiven Wurzeln.

Ist η speziell eine primitive $(p^f-1)^{\text{te}}$ Einheitswurzel, so sind also die (p^f-1) Potenzen

(4) $$1,\ \eta,\ \eta^2,\ \ldots\ \eta^{p^f-2}$$

voneinander verschiedene Wurzeln der Gleichung (1), und da diese nur (p^f-1) Wurzeln haben kann, so stellen sich alle Wurzeln dieser Gleichung als Potenzen von η dar. Es gilt also der Satz:

Ist η eine der $\varphi(p^f-1)$ primitiven $(p^f-1)^{\text{ten}}$ Einheitswurzeln, so ist jede andere $(p^f-1)^{\text{te}}$ Einheitswurzel als Potenz von η darstellbar, und für die Funktion $H_f(x)=x^{p^f}-x$ besteht also die folgende identische Zerlegung in ihre Linearfaktoren:

$$H_f(x)=x^{p^f}-x=x(x-1)(x-\eta)(x-\eta^2)\cdots(x-\eta^{p^f-2}).\quad (p)$$

Da hiernach bei der a. S. 186 (5) angegebenen Darstellung

(5) $$\beta=\eta^{(r)}\pi^r+\eta^{(r+1)}\pi^{r+1}+\cdots\qquad (\mathfrak{p})$$

der algebraischen Zahlen von $K(\alpha)$ für den Bereich von $\mathfrak{p}$ alle Koeffizienten $\eta^{(k)}$ entweder Null oder Potenzen von η sind, so ergibt sich endlich der Satz:

Jede algebraische Zahl β des Bereiches $K(\alpha)$ läßt sich für den Bereich eines beliebigen Primteilers $\mathfrak{p}$ auf eine einzige Weise in der Form (5) darstellen, und die hier auftretenden Koeffizienten $\eta^{(k)}$ sind entweder Null oder Potenzen einer primitiven $(p^f-1)^{\text{ten}}$ Einheitswurzel, wenn $\mathfrak{p}$ vom f^{ten} Grade ist.

Aus diesem Grunde soll der Körper $K(\eta)$ der primitiven $(p^f-1)^{\text{ten}}$ Einheitswurzeln der zu dem Primteiler $\mathfrak{p}$ gehörige Koeffizientenkörper genannt werden; dieser ist allein durch den Grad f von $\mathfrak{p}$ und die zugehörige Primzahl p völlig bestimmt.

§ 4. Die innerhalb $K(p)$ irreduktiblen Gleichungen für die $(p^f-1)^{\text{ten}}$ Einheitswurzeln.

Wie jede andere Zahl des Bereiches $K(p,\alpha)$ genügt auch die primitive Einheit η des Koeffizientenkörpers einer Gleichung des $\lambda=ef^{\text{ten}}$ Grades mit rationalen p-adischen Koeffizienten, deren linke Seite entweder selbst irreduktibel oder die Potenz einer irreduktiblen Funktion derselben Art ist. Ich will jetzt zeigen, daß diese Einheit η nebst den f Potenzen

(1) $$\eta,\ \eta^p,\ \eta^{p^2},\ \ldots\ \eta^{p^{f-1}}$$

einer irreduktiblen Gleichung f^{ten} Grades

(2) $$g(x)=(x-\eta)(x-\eta^p)\cdots(x-\eta^{p^{f-1}})=0\qquad (p)$$

mit rationalen p-adischen Koeffizienten genügt.

Zum Beweise denke ich mir die den Körper $K(\eta)$ bestimmende Funktion $H_f(x)$ in ihre irreduktiblen p-adischen Faktoren zerlegt; es sei:

(3) $$H_f(x) = x^{p^f} - x = g(x)\, g_1(x) \cdots g_{\nu-1}(x) \qquad (p)$$

diese Zerlegung. Da $D(H_f(x))$ durch p nicht teilbar ist, so sind auch die nullten Näherungswerte

(3a) $$g^{(0)}(x),\ g_1^{(0)}(x),\ \cdots\ g_{\nu-1}^{(0)}(x)$$

dieser Funktionen modulo p betrachtet irreduktibel und alle voneinander verschieden (vgl. S. 84 *)). Es sei nun η^k eine bestimmte Wurzel der Gleichung $H_f(x) = 0$; dann folgt aus der Zerlegung (3), daß η^k auch eine und nur eine der Gleichungen $g_i(x) = 0$ befriedigen muß. Ist nun etwa:

(4) $$g(\eta^k) = 0 \qquad (\mathfrak{p}),$$

so folgt durch Übergang zum nullten Näherungswerte, daß auch

(4a) $$g^{(0)}(\eta^k) \equiv 0 \pmod{\mathfrak{p}}$$

sein muß. Da aber die Diskriminante $D(g(x))$ durch p nicht teilbar ist, so ergibt sich auch umgekehrt aus (4a), daß η^k die Gleichung $g(x) = 0$ befriedigt; denn aus dieser Kongruenz folgt n. S. 155 unten für $\delta = 0$, daß die Gleichung $g(x) = 0$ eine Wurzel besitzen muß, welche modulo $\mathfrak{p}$ kongruent η^k ist; da aber diese Gleichung überhaupt nur Wurzeln η^l besitzt, und da alle diese modulo $\mathfrak{p}$ inkongruent sind, so besitzt in der Tat die Gleichung $g(x) = 0$ dann und nur dann eine bestimmte unter den Potenzen η^k als Wurzel, wenn $g^{(0)}(\eta^k)$ oder, was dasselbe besagt, wenn $g(\eta^k)$ selbst auch nur durch die erste Potenz von $\mathfrak{p}$ teilbar ist.

Hiernach ist es sehr leicht, diejenigen Einheitswurzeln aufzufinden, welche zu irgend einer Einheit η_0 für den Bereich von $\mathfrak{p}$ konjugiert sind. Es sei

(5) $$g(x) = 0$$

diejenige irreduktible Gleichung, deren Wurzel η_0 ist. Erhebt man dann die aus $g(\eta_0) = 0$ folgende Kongruenz:

(5a) $$g^{(0)}(\eta_0) \equiv 0 \pmod{\mathfrak{p}}$$

der Reihe nach zur p^{ten}, $(p^2)^{\text{ten}}, \ldots$ Potenz und beachtet den a. S. 78 (4a) bewiesenen Satz, so ergeben sich die Kongruenzen:

(5b) $$g^{(0)}(\eta_0^p) \equiv g^{(0)}(\eta_0^{p^2}) \equiv \cdots \equiv g^{(0)}(\eta_0^{p^{f-1}}) \equiv 0 \qquad \pmod{\mathfrak{p}};$$

die folgende Kongruenz fällt wieder mit der ersten (5a) zusammen, weil $\eta_0^{p^f} = \eta_0$ ist.

---

*) Endlich folgt aus (3) durch Übergang zu den Diskriminanten, daß auch die Diskriminanten aller ν Gleichungen $g_i(x) = 0$ p nicht enthalten, daß also in dem Koeffizientenkörper $K(\eta)$ p selbst eine Primzahl ist (s. S. 152 Mitte).

Ist also η_0 die Wurzel einer der irreduktiblen Gleichungen $g(x)=0$, so besitzt diese zugleich die Wurzeln $(\eta_0, \eta_0^p, \eta_0^{p^2}\ldots)$, und da sie keine mehrfachen Wurzeln haben kann, so sind alle diejenigen unter den obigen Einheitswurzeln, welche voneinander verschieden sind, einfache Wurzeln dieser Gleichung.

Es sei nun in der Reihe:

(6) $$\eta_0, \eta_0^p, \ldots \eta_0^{p^k}, \ldots \eta_0^{p^{k+f_0}}, \ldots$$

$\eta_0^{p^k}$ die erste Einheitswurzel, welche einer späteren $\eta_0^{p^{k+f_0}}$ gleich ist. Erhebt man dann in der Gleichung:

$$\eta_0^{p^k} = \eta_0^{p^{k+f_0}} \quad (\mathfrak{p})$$

beide Seiten zur $(p^{f-k})^{\text{ten}}$ Potenz und beachtet, daß $\eta_0^{p^f}=\eta_0$ ist, so ergibt sich:

(6a) $$\eta_0 = \eta_0^{p^{f_0}} \quad (\mathfrak{p}),$$

d. h. in der obigen Reihe (6) sind nur die ersten f_0 Potenzen voneinander verschieden, während

(6b) $$\eta_0^{p^{f_0}} = \eta_0, \quad \eta^{p^{f_0+1}} = \eta_0^p, \cdots \eta_0^{p^{f_0+l}} = \eta_0^{p^l}, \cdots$$

ist. In der unbegrenzten Reihe (6) wiederholen sich also die Elemente

(6c) $$\eta_0, \eta_0^p, \ldots \eta_0^{p^{f_0-1}}$$

in derselben Reihenfolge immer wieder, und diese sind alle verschieden. Hieraus folgt, daß eine Potenz $\eta_0^{p^{\bar{f}}}$ dann und nur dann gleich η_0 ist, wenn der Exponent $\bar{f}$ durch f_0 teilbar ist. Da nun für jedes η_0 $\eta_0^{p^f}=\eta_0$ ist, so muß jener kleinste Exponent f_0 stets ein Teiler von f sein.

Ich will nach einer von Herrn P. Bachmann herrührenden Bezeichnung sagen, eine Einheitswurzel η_0 paßt zum Exponenten f_0, wenn f_0 der kleinste Exponent ist, für den $\eta_0^{p^{f_0}}=\eta_0$ ist. Dann gilt also der Satz:

Jede Einheitswurzel η_0 paßt zu einem Exponenten f_0, welcher ein Teiler von f ist. Ist dann

(7) $$g_0(x) = 0$$

die irreduktible Gleichung mit rationalen p-adischen Koeffizienten, welcher η_0 genügt, so besitzt dieselbe Gleichung auch die konjugierten Wurzeln:

(7a) $$\eta_0, \eta_0^p, \eta_0^{p^2}, \ldots \eta_0^{p^{f_0-1}},$$

ihre linke Seite ist also durch das Produkt:

(7b) $$\bar{g}(x) = (x-\eta_0)(x-\eta_0^p)\cdots(x-\eta_0^{p^{f_0-1}}) = x^{f_0} + S_{f_0-1}x^{f_0-1} + \cdots + S_0$$

teilbar.

Man kann aber noch weiter gehen und beweisen, daß $g(x) = \bar{g}(x)$ sein muß, d. h. daß jene irreduktible Gleichung (7) nur den einen Wurzelzyklus $(\eta_0, \eta_0^p, \ldots \eta_0^{p^{f_0-1}})$ hat. Betrachtet man nämlich das entwickelte Produkt $\bar{g}(x)$ in (7b) nur modulo $\mathfrak{p}$, und beachtet dabei, daß jeder der hier auftretenden Koeffizienten S_i von x^i eine ganzzahlige symmetrische Funktion der f_0 Zahlen $\eta_0^{p^k}$ ist, so sieht man, daß jeder beliebige unter diesen Koeffizienten:

$$S_i = S_i(\eta_0, \eta_0^p, \ldots \eta_0^{p^{f_0-1}})$$

modulo $\mathfrak{p}$ einer der Zahlen $0, 1, \cdots p-1$ kongruent sein muß. In der Tat ist ja nach dem polynomischen Lehrsatze ebenso wie in (4a) a. S. 78:

$$S_i(\eta_0, \eta_0^p, \cdots \eta_0^{p^{f_0-1}})^p \equiv S_i(\eta_0^p, \eta_0^{p^2}, \ldots \eta_0) \equiv S_i(\eta_0, \ldots \eta_0^{p^{f_0-1}}) \pmod{\mathfrak{p}},$$

d. h. es genügt jene Zahl S_i der Kongruenz:

$$S_i^p - S_i \equiv S_i(S_i - 1) \cdots (S_i - \overline{p-1}) \equiv 0 \pmod{\mathfrak{p}},$$

woraus die Richtigkeit der letzten Behauptung unmittelbar hervorgeht. Also hat der nullte Näherungswert modulo $\mathfrak{p}$ von $\bar{g}(x)$ in (7b):

$$\bar{g}^{(0)}(x) = x^{f_0} + S_{f_0-1}^{(0)} x^{f_0-1} + \cdots + S_0^{(0)}$$

nur Zahlen der Reihe $0, 1, \cdots p-1$ als Koeffizienten. Enthielte nun $g(x)$ noch mehr Linearfaktoren als $\bar{g}(x)$, wäre also:

$$g(x) = \bar{g}(x)\,\bar{h}(x) \quad (\mathfrak{p}),$$

so ergäbe sich durch Übergang zu den nullten Näherungswerten:

$$g^{(0)}(x) \equiv \bar{g}^{(0)}(x)\,\bar{h}^{(0)}(x) \pmod{\mathfrak{p}},$$

also wegen S. 190 Anm. auch modulo p; d. h. auch $g^{(0)}(x)$ besäße modulo p betrachtet den ganzzahligen Faktor $g^{(0)}(x)$ von niedrigerem Grade, was nach der bei (3a) gemachten Bemerkung unmöglich ist.

Jede $(p^f - 1)^{\text{te}}$ Einheitswurzel η_0 genügt also nebst ihren f_0 konjugierten $(\eta_0, \eta_0^p, \ldots \eta_0^{p^{f_0-1}})$ einer irreduktiblen p-adischen rationalen Gleichung, deren Grad f_0 gleich dem Exponenten ist, zu dem η_0 paßt, und der stets gleich f oder gleich einem Teiler von f ist. Jede symmetrische Funktion dieser f_0 Einheitswurzeln ist eine rationale p-adische Zahl. Die Funktion $H_f(x)$ zerfällt für den Bereich von p in lauter Faktoren $g_i(x)$, deren Grad gleich f oder gleich einem Teiler von f ist.

Aus der Irreduktibilität der Gleichung mit den Wurzeln $\eta_0, \eta_0^p, \ldots \eta_0^{p^{f_0-1}}$ für den Bereich von p folgt nach dem a. S. 131 (5) bewiesenen Satze:

Jede Gleichung von beliebigem Grade:

$$G(\eta_0) = A_0 \eta_0^\varrho + A_1 \eta_0^{\varrho-1} + \cdots + A_\varrho = 0 \quad (\mathfrak{p})$$

mit rationalen p-adischen Koeffizienten bleibt richtig, wenn man η_0 der Reihe nach durch die konjugierten Zahlen

$$\eta_0, \eta_0^p, \ldots \eta_0^{p^{f_0-1}}$$

ersetzt.

Ist $\eta_0 = \eta$ speziell eine primitive Einheitswurzel, so paßt sie erst zum Exponenten f selber; denn wäre schon $\eta^{p^{f_0}} = \eta$ und wäre $f_0 < f$, so genügte ja η bereits der Gleichung $\eta^{p^{f_0}-1} = 1$, gehörte also sicher nicht zum Exponenten $(p^f - 1)$.

Jede $(p^f-1)^{\text{te}}$ Einheitswurzel η_0 gehört zu einem Exponenten d_0, einem Teiler von (p^f-1), nämlich dem kleinsten Exponenten, für den

$$\eta_0^{d_0} = 1 \tag{8}$$

ist; ferner paßt η_0 zu einem Exponenten f_0, einem Teiler von f nämlich dem kleinsten Exponenten, für den

$$\eta_0^{p^{f_0}} = \eta_0 \quad \text{also} \quad \eta_0^{p^{f_0}-1} = 1 \tag{8a}$$

ist. Diese beiden Exponenten stehen in einer sehr einfachen Beziehung: offenbar folgt nämlich aus (8) und (8a), daß f_0 der kleinste Exponent sein muß für den:

$$p^{f_0} \equiv 1 \pmod{d_0} \tag{8b}$$

ist, d. h. es besteht der Satz:

Sind d_0 und f_0 die beiden Exponenten zu denen eine und dieselbe Einheitswurzel η_0 gehört, bzw. paßt, so ist f_0 der Exponent, zu dem die Primzahl p modulo d_0 gehört.

Ich wende die bisher gefundenen Resultate auf den einfachsten Fall an, daß die den Körper $K(\alpha)$ definierende ganzzahlige Gleichung n^{ten} Grades $F(x) = 0$ für den Primzahlmodul p irreduktibel ist, d. h, daß der nullte Näherungswert $F^{(0)}(x)$ modulo p nicht in Faktoren niedrigeren Grades zerfällt. Alsdann ist $F(x)$ nach S. 79 unten auch für den Bereich dieser Primzahl also a fortiori auch absolut irreduktibel; es ist also in diesem Falle $n = \lambda = ef$. Ferner ist die Gleichungsdiskriminante durch p nicht teilbar, also ist nach dem a. S. 152 Mitte bewiesenen Satze p für den Körper $K(\alpha)$ selbst eine Primzahl, d. h. es ist $e = 1$, mithin $n = f$. Die f Wurzeln $\varepsilon, \varepsilon_1, \ldots \varepsilon_{f-1}$ dieser Gleichung

$$F(x) = x^f + a_1 x^{f-1} + \cdots + a_f = 0 \quad (p) \tag{9}$$

für den Bereich von p bilden also einen einzigen Wurzelzyklus. Es sei:

$$\varepsilon = \eta_0 + \eta_1 p + \eta_2 p^2 + \cdots$$

die eine von diesen f Wurzeln; dann sind die Koeffizienten η_i entweder Null oder eindeutig bestimmte $(p^f-1)^{\text{te}}$ Einheitswurzeln, welche alle in der Form:

$$\eta_i = \eta^{k_i}$$

dargestellt werden können, wenn η eine primitive $(p^f-1)^{\text{te}}$ Einheitswurzel ist, und die k_i ganzzahlige Exponenten bedeuten. Also läßt sich ε auch in der Form schreiben:

$$\varepsilon = \varphi(\eta),$$

wo $\varphi(\eta)$ eine ganze Funktion von η mit ganzzahligen p-adischen Koeffizienten bedeutet. Da nun die Gleichung

$$0 = F(\varepsilon) = F(\varphi(\eta))$$

nach dem a. S. 193 oben bewiesenen Satze richtig bleibt, wenn man η durch $\eta^p, \eta^{p^2}, \ldots \eta^{p^{f-1}}$ ersetzt, so besitzt die Gleichung (9) außer ε auch alle Wurzeln, welche aus ε dadurch hervorgehen, daß man in den Koeffizienten $\eta_i = \eta^{k_i}$ η allgemein durch η^{p^r} ersetzt. Da aber durch diese Substitution

$$\eta_i = \eta^{k_i} \text{ übergeht in } \eta^{p^r \cdot k_i} = \eta_i^{p^r},$$

so ergibt sich, daß die Gleichung (9) den folgenden Zyklus von p-adischen Wurzeln besitzt:

$$\begin{aligned}
\varepsilon &= \eta_0 + \eta_1 p + \eta_2 p^2 + \cdots, \\
\varepsilon_1 &= \eta_0^p + \eta_1^p p + \eta_2^p p^2 + \cdots, \\
\varepsilon_2 &= \eta_0^{p^2} + \eta_1^{p^2} p + \eta_2^{p^2} p^2 + \cdots, \\
&\vdots \\
\varepsilon_{f-1} &= \eta_0^{p^{f-1}} + \eta_1^{p^{f-1}} p + \eta_2^{p^{f-1}} p^2 + \cdots.
\end{aligned} \tag{10} \quad (p)$$

Da ferner die aus diesen Zahlen gebildete Funktion

$$(x-\varepsilon)(x-\varepsilon_1)\cdots(x-\varepsilon_{f-1})$$

als symmetrische Funktion der konjugierten Einheitswurzeln

$$(\eta, \eta^p, \ldots \eta^{p^{f-1}})$$

rationale p-adische Koeffizienten besitzt und mit der für den Bereich von p irreduktiblen Funktion $F(x)$ in (9) einen gemeinsamen Teiler hat, nämlich den Linearfaktor $x-\varepsilon$, so muß

$$F(x) = (x-\varepsilon)(x-\varepsilon_1)\cdots(x-\varepsilon_{f-1}) \tag{11}$$

sein; jene f p-adischen Zahlen sind also sämtlich voneinander verschieden und bilden eben den zu p gehörigen Wurzelzyklus der Gleichung (9). Es ergibt sich also der Satz:

Die Wurzeln einer jeden Gleichung f^{ten} Grades:

$$F(x) = 0 \qquad (p),$$

deren linke Seite auch modulo p irreduktibel ist, können allein durch $(p^f-1)^{\text{te}}$ Einheitswurzeln vollständig dargestellt werden.

Für den zugehörigen Körper $K(\varepsilon)$ ist also p selbst eine Primzahl, und der Körper $K(p, \varepsilon)$ ist mit dem Koeffizientenkörper $K(p, \eta)$ identisch.

In Zukunft will ich die zu:

$$\varepsilon = \eta_0 + \eta_1 p + \eta_2 p^2 + \cdots$$

konjugierten Reihen (10)

$$\eta_0^{p^k} + \eta_1^{p^k} p + \eta_2^{p^k} p^2 + \cdots \qquad (k = 1, 2, \cdots f-1),$$

welche aus ε dadurch hervorgehen, daß man jeden der Koeffizienten η_i durch seine $p^{k\text{te}}$ Potenz ersetzt, mitunter durch $\varepsilon^{(p^k)}$ bezeichnen. Dann besitzt also die Gleichung (9) die folgenden f konjugierten Wurzeln:

(12) $$\varepsilon,\ \varepsilon^{(p)},\ \varepsilon^{(p^2)},\ \ldots\ \varepsilon^{(p^{f-1})},$$

und es ist stets $\varepsilon^{(p^f)} = \varepsilon$.

Die f Wurzeln einer solchen Gleichung sind modulo p betrachtet kongruent den Anfangsgliedern:

(13) $$\eta_0,\ \eta_0^p,\ \ldots\ \eta_0^{p^{f-1}}$$

der Reihen (10), und zwar paßt hier η_0 zum Exponenten f selbst und nicht zu einem Teiler von f, weil anderenfalles zwei unter den Zahlen (13) modulo p kongruent wären, was mit der Irreduktibilität von $F(x)$ modulo p im Widerspruch stehen würde. Hieraus folgt nach S. 190 oben, daß der nullte Näherungswert der Grundgleichung:

(13a) $$F^{(0)}(x) \equiv (x - \eta_0)(x - \eta_0^p) \cdots (x - \eta_0^{p^{f-1}}) \pmod{p},$$

d. h. modulo p kongruent einem der irreduktiblen Faktoren f^{ten} Grades ist, in welche die Funktion $x^{p^f} - x$ modulo p zerfällt; und da nur vorausgesetzt war, daß $F^{(0)}(x)$ irgend eine modulo p irreduktible Funktion f^{ten} Grades sein sollte, so folgt, daß $x^{p^f} - x$ modulo p betrachtet durch alle für diesen Modul irreduktiblen Funktionen vom f^{ten} Grade teilbar ist. Ist aber ferner f_0 irgend ein Teiler von $f = f_0 \bar{f}_1$, und

$$\bar{g}(x) = x^{f_0} + g_1 x^{f_0 - 1} + \cdots + g_{f_0}$$

irgend eine modulo p irreduktible Funktion des f_0^{ten} Grades, so ist aus demselben Grunde $\bar{g}(x)$ modulo p betrachtet ein einfacher Teiler von $x^{p^{f_0}} - x$; und da $x^{p^f} - x$ wiederum durch $x^{p^{f_0}} - x$ teilbar ist, weil ja $(p^{f_0} - 1)$ ein Teiler von $p^f - 1$, also jede $(p^{f_0} - 1)^{\text{te}}$ Wurzel der Einheit auch eine $(p^f - 1)^{\text{te}}$ Einheitswurzel ist, so folgt, daß $\bar{g}(x)$ modulo p betrachtet auch ein einfacher Teiler von $x^{p^f} - x$ ist. Da endlich $x^{p^f} - x$ modulo p betrachtet nach dem a. S. 192 unten bewiesenen Satze auch keine anderen irreduktiblen Faktoren enthält, als solche, deren Grad gleich f oder gleich einem Teiler von f ist, so ergibt sich der folgende merkwürdige Satz:

Die Funktion $x^{p^f} - x$ ist modulo p kongruent dem Produkte aller und nur der modulo p irreduktiblen ganzzahligen Funktionen, deren Grad gleich f oder gleich einem Teiler von f ist.

So besteht z. B. für $f = 1$ die Zerlegung:

$$x^p - x \equiv x(x-1)\cdots(x - \overline{p-1}) \quad (\text{mod.}\ p),$$

und die rechts stehenden Linearfaktoren sind ja in der Tat alle modulo p inkongruenten Funktionen ersten Grades. Ferner ist für $f = 2$, $p = 2$:

$$x^{2^2} - x = x^4 - x \equiv (x^2 + x + 1)(x+1)\,x \quad (\text{mod.}\ 2),$$

d. h. $x^2 + x + 1$ ist die einzige modulo 2 irreduktible Funktion zweiten Grades. Für $f = 3$, $p = 2$ ergibt sich leicht:

$$x^{2^3} - x = x^8 - x \equiv (x^3 + x^2 + 1)(x^3 + x + 1)(x+1)\,x \quad (\text{mod}\ 2).$$

Endlich erhält man für $f = 4$, $p = 2$ die Zerlegung:

$$x^{2^4} - x = x^{16} - x \equiv (x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + 1)(x^4 + x + 1)$$
$$(x^2 + x + 1)(x+1)\,x \quad (\text{mod.}\ 2),$$

und die sechs rechts stehenden Faktoren sind die einzigen modulo 2 inkongruenten irreduktiblen Funktionen vierten, zweiten und ersten Grades.

§ 5. Die für den Bereich von $\mathfrak{p}$ äquivalenten Primzahlen π von $K(\alpha)$.

Die soeben durchgeführten Betrachtungen zeigen, daß der Körper $K(\eta)$ der $(p^f - 1)^{\text{ten}}$ Wurzeln der Einheit nebst den zu ihm gehörigen p-adischen Zahlen:

$$\varepsilon = \eta_0 + \eta_1 p + \cdots$$

genügt, um alle auch modulo p irreduktiblen Gleichungen für den Bereich von p zu lösen, deren Grad gleich f oder gleich einem Teiler von f ist. Aber auch für die Untersuchung eines algebraischen Körpers $K(\alpha)$ vom n^{ten} Grade in bezug auf einen beliebigen Primteiler $\mathfrak{p}$ von p von der e^{ten} Ordnung und vom f^{ten} Grade ist jener Koeffizientenkörper $K(\eta)$ von fundamentaler Bedeutung.

Ich beweise jetzt nämlich, daß jede zu $\mathfrak{p}$ gehörige Primzahl π für den Bereich von $\mathfrak{p}$ einer irreduktiblen Eisensteinschen Gleichung e^{ten} Grades

(1) $$\psi(\pi) = \pi^e + p c_{e-1} \pi^{e-1} + \cdots + p c_0 = 0 \quad (\mathfrak{p})$$

genügt, deren Koeffizienten c_i ganze p-adische Zahlen des Koeffizientenkörpers $K(\eta)$ sind, und deren letzter Koeffizient c_0 durch p nicht mehr teilbar ist.

Dies folgt unmittelbar daraus, daß $\pi^e = p\varepsilon$ für den Bereich von $\mathfrak{p}$ gleich einer genau durch p teilbaren Zahl von $K(\alpha)$ ist, daß also für π eine Gleichung

$$(2)\qquad \pi^e = p(\eta_0 + \eta_1\pi + \cdots + \eta_{e-1}\pi^{e-1} + p\varepsilon_1) \qquad (\mathfrak{p})$$

besteht, in welcher alle Koeffizienten η_i Einheitswurzeln bedeuten, und wo $\eta_0 \gtrless 0$ ist; hier wird eben das Aggregat aller auf $\eta_{e-1}\pi^{e-1}$ folgenden Glieder, welche ja alle p enthalten, durch $p\varepsilon_1$ bezeichnet. Schreibt man nun wieder ε_1 in derselben Form

$$\varepsilon_1 = \eta_0' + \eta_1'\pi + \cdots + \eta_{e-1}'\pi^{e-1} + p\varepsilon_2$$

und fährt so fort, so erhält man eine Reihe von Gleichungen:

$$(3)\qquad \begin{aligned} \pi^e &= p\eta_{e-1}\pi^{e-1} + p\eta_{e-2}\pi^{e-2} + \cdots + p\eta_0 + p^2\varepsilon_1, \\ p^2\varepsilon_1 &= p^2\eta_{e-1}'\pi^{e-1} + p^2\eta_{e-2}'\pi^{e-2} + \cdots + p^2\eta_0' + p^3\varepsilon_2, \\ p^3\varepsilon_2 &= p^3\eta_{e-1}''\pi^{e-1} + p^3\eta_{e-2}''\pi^{e-2} + \cdots + p^3\eta_0'' + p^4\varepsilon_3, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots . \end{aligned}$$

Addiert man diese Gleichungen, läßt dann die links und rechts stehenden Glieder $p^i\varepsilon_{i-1}$ fort, und bezeichnet die dann sich ergebenden Koeffizienten von $\pi^{e-1}, \pi^{e-2}, \ldots 1$, welche ja offenbar sämtlich p-adische Zahlen von $K(\eta)$ und Multipla von p sind, bzw. durch $-pc_{e-1}, -pc_{e-2}, \cdots -pc_0$, so ergibt sich für π in der Tat die obige Gleichung (1). In ihr ist das letzte Glied

$$pc_0 = -p(\eta_0 + \eta_0' p + \cdots)$$

eine genau durch p teilbare p-adische Zahl von $K(\eta)$, da das Anfangsglied η_0 sicher eine Einheit ist.

Die Gleichung (1) für π ist für den Bereich der p-adischen Zahlen von $K(\eta)$ irreduktibel, da ihre linke Seite eine Eisensteinsche Funktion ist und ihr konstantes Glied nur die erste Potenz von p als Teiler besitzt. (S. S. 76 oben).

Umgekehrt wird durch jede Eisensteinsche Gleichung

$$(4)\qquad \psi(x) = x^e + pc_{e-1}x^{e-1} + \cdots + pc_0 = 0 \qquad (p),$$

deren Koeffizienten c_i ganze Zahlen eines beliebigen Koeffizientenkörpers $K(\eta)$ sind, und deren konstantes Glied pc_0 nur durch die erste Potenz von p teilbar ist, stets eine e^{te} Wurzel aus p definiert; denn setzt man $x = p^{\frac{1}{e}}\varepsilon$ in $\psi(x)$ ein und dividiert die linke Seite durch p, so findet man, daß die algebraische Größe ε der Gleichung:

$$(4\text{a})\quad \varepsilon^e + p^{\frac{e-1}{e}}c_{e-1}\varepsilon^{e-1} + p^{\frac{e-2}{e}}c_{e-2}\varepsilon^{e-2} + \cdots + p^{\frac{1}{e}}c_1\varepsilon + c_0 = 0 \qquad (p)$$

genügt, d. h. ε ist wirklich eine algebraische Einheit modulo p, da alle Gleichungskoeffizienten in (4a) ganze algebraische Zahlen sind,

und das konstante Glied c_0 eine Einheit ist. Wählt man in der Gleichung (4) für x irgend eine genau durch $\mathfrak{p} \sim p^{\frac{1}{e}}$ teilbare Zahl, so ist jedes Glied $p^k \eta_i^{(k)} x^i$ von $\psi(x)$ genau durch die Potenz $\mathfrak{p}^{ke+i} \sim p^{k+\frac{i}{e}}$ von $\mathfrak{p}$ teilbar, deren Exponent die Ordnungszahl dieses Gliedes heißen soll. Alle diese Ordnungszahlen sind voneinander verschieden mit Ausnahme der beiden Glieder x^e und des Anfangsgliedes $pc_0^{(0)}$ von pc_0, welche beide die niedrigste Ordnungszahl e besitzen.

Unter einem Näherungswerte der $(\varrho^{(0)})^{\text{ten}}$ Ordnung von $\psi(x)$ verstehe ich die Funktion $\psi_0(x)$, welche aus allen Gliedern von $\psi(x)$ besteht, deren Ordnungszahlen gleich oder kleiner als $\varrho^{(0)}$ sind, so daß also für jedes $x \sim p^{\frac{1}{e}}$

(5) $$\psi(x) \equiv \psi_0(x) \pmod{\mathfrak{p}^{\varrho^{(0)}+1}}$$

ist.

Auch hier will ich nun die Wurzeln der irreduktiblen Gleichung (1) mit p-adischen Koeffizienten von $K(\eta)$ dadurch mit jeder vorgegebenen Genauigkeit berechnen, daß ich an ihrer Stelle eine Näherungsgleichung:

(6) $$\psi_0(x) = x^e + pc_{e-1}^{(0)} x^{e-1} + \cdots + pc_1^{(0)} x + pc_0^{(0)} = 0$$

betrachte, deren linke Seite ein Näherungswert von $\psi(x)$ von einer gleich anzugebenden genügend hohen Ordnung $\varrho^{(0)}$ ist. Ich benutze dazu die a. S. 72 flgde. auseinandergesetzte Newtonsche Annäherungsmethode für p-adische Gleichungen. Der dort geführte Beweis bezog sich zwar zunächst nur auf Gleichungen mit rationalen p-adischen Zahlkoeffizienten und ebensolchen Wurzeln, aber ein Blick auf ihn läßt erkennen, daß er ohne jede Änderung auch für den hier betrachteten Fall anwendbar ist, wo die Koeffizienten und Wurzeln algebraische p-adische Zahlen des Körpers $K(\alpha)$ sind; nur tritt hier natürlich an die Stelle der Primzahl p der zu $K(\alpha)$ gehörige Primdivisor $\mathfrak{p}$.

Um nun die Newtonsche Näherungsmethode auf die Gleichung (1) anzuwenden, definiere ich den ersten Näherungswert π_0 von π als eine Wurzel der algebraischen Gleichung (6). Dann besteht also für ein variables $x \sim p^{\frac{1}{e}}$ die Kongruenz (5). Ich wähle nun zunächst $\varrho^{(0)} \geq e$; dann ist auch in $\psi_0(x)$ das Endglied $pc_0^{(0)}$ von Null verschieden und genau durch $p \sim \mathfrak{p}^e$ teilbar; also ist auch $\psi_0(x)$ in (6). eine Eisensteinsche Funktion, und der durch die Näherungsgleichung (6) definierte Näherungswert π_0 von π ist sicher ebenfalls äquivalent $p^{\frac{1}{e}}$. Setzt

man ferner in der Kongruenz (5) $x = \pi_0$, wodurch die rechte Seite verschwindet, so wird sicher:

(6a) $$\psi(\pi_0) \equiv 0 \pmod{\mathfrak{p}^{\varrho^{(0)}+1}}.$$

Ich will nun die noch zur Verfügung stehende Zahl $\varrho^{(0)}$ so groß wählen daß das Newtonsche Annäherungsverfahren anwendbar wird. Zu diesem Zwecke bilde ich nach der a. S. 72 unten gegebenen Vorschrift die Ableitungen:

(7) $$\psi'(x), \quad \frac{\psi''(x)}{2!}, \quad \frac{\psi'''(x)}{3!}, \ldots \frac{\psi^{(e)}(x)}{e!},$$

setze in ihnen $x = \pi_0 \sim p^{\frac{1}{e}}$ und bestimme ihre Ordnungszahlen

(7a) $$\varrho', \quad \varrho'', \quad \varrho''', \ldots \varrho^{(e)}.$$

Diese Ordnungszahlen können hier sehr leicht gefunden werden. Es ist nämlich:

(7b) $$\begin{aligned} \psi'(\pi_0) &= e\pi_0^{e-1} + (e-1)\, pc_{e-1}\pi_0^{e-2} + \cdots + pc_1, \\ \frac{\psi''(\pi_0)}{1 \cdot 2} &= e_2\pi_0^{e-2} + (e-1)_2\, pc_{e-1}\pi_0^{e-3} + \cdots + pc_2, \\ &\vdots \\ \frac{\psi^{(e)}(\pi_0)}{e!} &= 1, \end{aligned}$$

wo allgemein r_k den k^{ten} Binomialkoeffizienten von r bedeutet.

Alle rechtsstehenden Summen sind so beschaffen, daß keine zwei Summanden einer und derselben Zahl $\frac{\psi^{(i)}(\pi_0)}{i!}$ die gleiche Ordnungszahl haben, da alle diese Ableitungen ganze Funktionen von $\pi_0 \sim p^{\frac{1}{e}}$ von niedrigerem als dem e^{ten} Grade sind, deren Koeffizienten nur ganzzahlige Potenzen von p enthalten. Niemals können sich also in einer solchen Summe zwei Summanden aufheben, da sie alle mit verschiedenen Potenzen von $p^{\frac{1}{e}}$ beginnen. Jede dieser e Zahlen $\frac{\psi^{(i)}(\pi_0)}{i!}$ besitzt also in bezug auf den Primteiler $\mathfrak{p} \sim p^{\frac{1}{e}}$ die Ordnungszahl $\varrho^{(i)}$ ihres niedrigsten Gliedes; diese ist mithin sehr leicht festzustellen. Ferner folgt aus derselben Überlegung, daß die Ordnungszahlen $\varrho', \varrho'', \ldots \varrho^{(e)}$ ungeändert bleiben, wenn man den ersten Näherungswert π_0 durch einen folgenden π_0' ersetzt, da ja auch dieser äquivalent $p^{\frac{1}{e}}$ ist. Speziell ist die letzte Ordnungszahl $\varrho^{(e)}$ offenbar gleich Null, während für alle übrigen Ordnungszahlen $\varrho^{(i)}$ die Ungleichungen:

(8) $$\varrho^{(i)} \geqq e - i \qquad (i = 1, 2, \cdots e-1)$$

erfüllt sind, da ja allgemein das Anfangsglied $e_i \pi_0^{e-i}$ von $\frac{\psi^{(i)}(\pi_0)}{i!}$ mindestens durch $\mathfrak{p}^{e-i}$, alle anderen Glieder aber mindestens durch $p \sim \mathfrak{p}^e$ teilbar sind.

Ich wähle nun als Ordnungszahl $\varrho^{(0)}$ des Näherungswertes $\psi_0(x)$ von $\psi(x)$ die kleinste ganze Zahl, welche die beiden Bedingungen erfüllt:

$$\varrho^{(0)} \geqq e, \tag{9}$$

$$\varrho^{(0)} + 1 > \mathrm{Max}\left(\frac{2\varrho' - \varrho''}{1}, \frac{3\varrho' - \varrho'''}{2}, \dots \frac{e\varrho' - \varrho^{(e)}}{e-1}\right). \tag{10}$$

Dann folgt aus der ersten Bedingung, daß der Näherungswert $\pi_0 \sim p^{\frac{1}{e}}$ ist, und aus der zweiten, nach (7a) a. S. 73, (wobei zu beachten ist, daß hier $\varrho^{(0)} + 1$ an die Stelle von ϱ getreten ist), daß die Anwendung des Newton'schen Verfahrens einen genaueren Näherungswert

$$\pi_0' = \pi_0 + h$$

liefert, wo

$$h = -\frac{\psi_0(\pi_0)}{\psi_0'(\pi_0)}$$

mindestens die Ordnungszahl $\varrho^{(0)} + 1 - \varrho'$ hat, und diese ist sicher größer als 1, also mindestens gleich 2. In der Tat liefert ja die letzte Bedingung von (10) unter Berücksichtigung von (8) die Ungleichung:

$$\varrho^{(0)} + 1 > \frac{e\varrho'}{e-1}, \quad \text{also} \quad \varrho^{(0)} + 1 - \varrho' > \frac{\varrho'}{e-1} \geqq 1.$$

Die Fortsetzung dieses Verfahrens liefert also für π eine Entwicklung von der Form:

$$\pi = \pi_0 + \eta_2 \pi_0^2 + \eta_3 \pi_0^3 + \cdots \quad (\mathfrak{p}),$$

und die Auflösung dieser Gleichung nach π_0 eine Darstellung:

$$\pi_0 = \pi + \bar{\eta}_2 \pi^2 + \bar{\eta}_3 \pi^3 + \cdots \quad (\mathfrak{p}),$$

von π_0 durch π, in welcher $\bar{\eta}_2, \bar{\eta}_3, \dots$ wohlbestimmte $(p^f - 1)^{\text{te}}$ Wurzeln der Einheit oder Null sind; also ist die durch die Gleichung $\psi_0(x) = 0$ definierte gewöhnliche algebraische Zahl π_0 in der Tat eine zu π äquivalente Primzahl des Körpers $K(p, \alpha)$. Den so gewonnenen wichtigen Satz spreche ich in der folgenden Form aus:

Ist

$$\psi(x) = 0 \quad (\mathfrak{p}) \tag{11}$$

die Gleichung, welcher irgend eine Primzahl des Körpers $K(\alpha)$ genügt, und besitzen die e Zahlen:

$$\frac{\psi'(\pi)}{1}, \frac{\psi''(\pi)}{2!}, \dots \frac{\psi^{(e)}(\pi)}{e!} \tag{11a}$$

bzw. die Ordnungszahlen $\varrho', \varrho'', \ldots \varrho^{(e)}$, so kann man an Stelle der Gleichung (11) ihren $\varrho^{(0)\text{-ten}}$ Näherungswert

$$\psi^{(0)}(x) = 0 \tag{11b}$$

zur Definition der Primzahl jenes Bereiches benutzen, wenn die Ordnungszahl $\varrho^{(0)}$ die kleinste ganze Zahl ist, für welche

$$\varrho^{(0)} + 1 > \operatorname{Max}\left(\frac{2\varrho' - \varrho''}{1}, \quad \frac{3\varrho' - \varrho'''}{2}, \ldots \frac{e\varrho' - \varrho^{(e)}}{e-1}\right) \tag{11c}$$

ist.

In diesem Satze konnte die erste Bedingung $\varrho^{(0)} \geqq e$ in (9) fortgelassen werden, da sie in der zweiten enthalten ist; in der Tat folgt sie aus

$$\varrho^{(0)} + 1 > \frac{e\varrho' - \varrho^{(e)}}{e-1},$$

da $\varrho^{(e)} = 0, \quad \varrho' \geqq e - 1$ ist.

§ 6. Die einfachsten Gleichungen für die Primzahlen π innerhalb des Koeffizientenkörpers $K(\eta)$.

Im allgemeinen wird nun die Gleichung:

$$\psi_0(x) = x^e + pc_{e-1}^{(0)} x^{e-1} + \cdots + pc_0^{(0)} = 0,$$

welche wir zur Definition der Primzahl π_0 wählen können, ganz außerordentlich einfach; sie reduziert sich nämlich auf eine reine Gleichung:

$$x^e - p\eta_0 = 0, \tag{1}$$

wo η_0 eine von der Natur des betreffenden Primteilers abhängige $(p^f - 1)^{\text{te}}$ Einheitswurzel ist. Und zwar ist diese äußerste Vereinfachung der Gleichung für π_0 nur in dem ganz singulären Falle nicht möglich, wenn e, d. h. die Ordnung des Primteilers $\mathfrak{p}$ durch die Primzahl p selbst teilbar ist. Da $ef = \lambda \leqq n$ ist, so kann dieser Ausnahmefall überhaupt nur für sehr wenige Primzahlen vorkommen, welche kleiner als der Grad der Grundgleichung sind. Aber gerade diese ganz singulären Fälle zeigten bisher bei der Untersuchung Anomalieen, welche mit Hilfe der früheren Theorieen nicht zu beseitigen waren, während bei dem hier befolgten Verfahren niemals eine Ausnahme für die später abzuleitenden Resultate vorkommen wird.

Von der größten Wichtigkeit ist aber der zunächst zu betrachtende Normalfall, daß e durch p nicht teilbar ist. Es sei in der Gleichung für π:

$$\psi(x) = x^e + pc_{e-1}x^{e-1} + \cdots + pc_0 = 0$$

e kein Multiplum von p; dann ist zunächst die Ordnungszahl ϱ' der ersten Ableitung:

$$\psi'(\pi) = e\pi^{e-1} + pc_{e-1}(e-1)\pi^{e-2} + \cdots + pc_1$$

genau gleich $e-1$, da das erste Glied diese Ordnungszahl hat und alle folgenden mindestens durch $p \sim \mathfrak{p}^e$ teilbar sind. Genau ebenso folgt allgemein, daß die Ordnungszahl $\varrho^{(i)}$ von

$$\frac{\psi^{(i)}(\pi)}{i!} = e_i\pi^{e-i} + pc_{e-1}(e-1)_i\pi^{e-i-1} + \cdots$$

gleich oder größer als $e-i$ ist.

Also ist in diesem Falle allgemein:

$$\frac{i\varrho' - \varrho^{(i)}}{i-1} \leqq \frac{i(e-1)-(e-i)}{i-1} = e.$$

Wählt man also für $\psi_0(x)$ den e^{ten} Näherungswert von $\psi(x)$, so folgt aus (11c) a. vor. S., daß die durch die Gleichung $\psi_0(x) = 0$ definierte Zahl π_0 ebenfalls eine Primzahl modulo $\mathfrak{p}$ für den Bereich von $K(\alpha)$ ist. Nun sind aber in $\psi(x)$ alle Koeffizienten außer dem von x^e und dem Anfangsglied von pc_0 von höherer als der e^{ten} Ordnung; bezeichnet man also dieses letztere Glied mit $-p\eta_0$, wo η_0 eine eindeutig bestimmte $(p^f-1)^{\text{te}}$ Einheitswurzel ist, so genügt in diesem Falle wirklich die Entwicklungszahl π_0 der reinen Gleichung:

$$\pi_0^e - p\eta_0 = 0 \quad (p)$$

w. z. b. w.

Auch die $(p^f-1)^{\text{te}}$ Einheitswurzel η_0, welche in dieser reinen Gleichung als Koeffizient von p auftritt, kann noch wesentlich reduziert werden. Es sei η eine primitive $(p^f-1)^{\text{te}}$ Einheitswurzel und

$$\eta_0 = \eta^{k_0}.$$

Ersetzt man dann π_0 durch die äquivalente Primzahl:

$$\bar{\pi} = \eta^k\pi_0,$$

so genügt $\bar{\pi}$ offenbar der reinen Gleichung:

$$\bar{\pi}^e = \eta^{k_0+ek}p = \eta^{k_0+ek+(p^f-1)k'}\cdot p, \tag{2}$$

wo k und k' ganz beliebig angenommen werden können, da $\eta^{(p^f-1)k'}$ stets gleich 1 ist. Es sei nun

$$e_0 = (e, p^f-1)$$

der größte gemeinsame Teiler von e und (p^f-1), dann kann man k und k' stets so bestimmen, daß $ek + (p^f-1)k' = \mu e_0$ ein beliebiges Multiplum von e_0 wird. Wir können nun diesen Multiplikator μ auf eine einzige Art so wählen, daß der Exponent von η in (2) nicht negativ und kleiner als e_0 wird. Bezeichnen wir diese eindeutig bestimmte Primzahl $\bar{\pi}$ jetzt durch π, so ergibt sich der folgende interessante Satz:

Ist $\mathfrak{p}$ ein Primteiler einer reellen Primzahl p vom Grade f und der Ordnung e, und ist e durch p nicht teilbar, so existiert in dem Körper $K(\alpha)$ stets eine zu $\mathfrak{p}$ gehörige Primzahl π, welche der reinen Gleichung:

(3) $$\pi^e = \eta^{k_0} p$$

genügt; hier bedeutet η eine primitive $(p^f - 1)^{\text{te}}$ Einheitswurzel, ferner k_0 eine der Zahlen $(0, 1, 2, \ldots e_0 - 1)$, und endlich ist:

(3a) $$e_0 = (e, p^f - 1).$$

Im wesentlichen ist also π gleich $p^{\frac{1}{e}}$, aber im allgemeinen tritt eben noch jene Einheitswurzel η^{k_0} hinzu, welche durch eine veränderte Wahl von π, wie wir sehen, nicht fortzuschaffen ist. Nur dann wird jene Einheit immer fehlen, wenn e und $(p^f - 1)$ teilerfremd, wenn also $e_0 = 1$ ist. Die Anzahl der in diesem Sinne nicht aufeinander reduzierbaren Körper $K(p, \alpha)$ ist also gleich dem größten gemeinsamen Teiler von e und $p^f - 1$, falls e durch p nicht teilbar ist.

Ich betrachte jetzt den allgemeinsten Fall, daß die Ordnung e des Primteilers $\mathfrak{p}$ durch eine beliebig hohe Potenz von p teilbar ist; es sei:

(4) $$e = p^s e_0.$$

Dann zeige ich, daß man die Gleichung des $(p^s e_0)^{\text{ten}}$ Grades für π auf die Auflösung einer reinen Gleichung des Grades e_0 in dem Körper $K(\eta)$ und einer Gleichung vom $(p^s)^{\text{ten}}$ Grade reduzieren kann. Zu diesem Zwecke betrachte ich neben der Primzahl π ihre $(p^s)^{\text{te}}$ Potenz:

(5) $$\pi^{p^s} = \Pi.$$

Führt man dann in die Gleichung für π:

(6) $$\psi(\pi) = \pi^e + p c_{e-1} \pi^{e-1} + \cdots + p c_0 = 0$$

diese Primzahlpotenz Π ein, so läßt sich jede in ihr auftretende Potenz von π in der Form schreiben:

$$\pi^k = \pi^{p^s k_0 + l_0} = \Pi^{k_0} \pi^{l_0},$$

wo $k_0 \leqq e_0$, $l_0 < p^s$ ist. Ordnet man die so sich ergebende Gleichung nach Potenzen von Π, so erhält man für Π eine Gleichung:

(6a) $$\Psi(\Pi) = \Pi^{e_0} + p C_{e_0 - 1} \Pi^{e_0 - 1} + \cdots + p C_1 \Pi + p C_0 = 0,$$

wo die Koeffizienten C_i offenbar die folgende Form haben:

(6b) $$C_i = c_0^{(i)} + c_1^{(i)} \pi + \cdots + c_{p^s - 1}^{(i)} \pi^{p^s - 1},$$

und wo C_0 wieder eine Einheit ist, da ihr Anfangsglied gleich c_0 in der Gleichung (6) für π ist. Also genügt $\Pi = \pi^{p^f}$ zunächst der Eisensteinschen Gleichung vom Grade e_0:

$$\text{(6c)} \qquad \Psi(X) = X^{e_0} + pC_{e_0-1}X^{e_0-1} + \cdots + pC_0 = 0,$$

deren sämtliche Koeffizienten C_i ganze algebraische Zahlen des Körpers $K(\varepsilon, \pi)$ sind, und in deren letztem Gliede C_0 eine Einheit modulo $\mathfrak{p}$ ist.

Ich führe nun zur Auflösung dieser Gleichung eine Wurzel Π_0 der Näherungsgleichung:

$$\text{(7)} \qquad \Psi^{(0)}(X) = X^{e_0} + pc_0^{(0)} = 0$$

ein, wo $c_0^{(0)}$ den nullten Näherungswert von C_0, also das Anfangsglied von c_0 in $\psi(x)$ bedeutet. Dann ist auch $\Pi_0 \sim \Pi \sim p^{\frac{1}{e_0}}$, und man zeigt genau wie vorher, daß man durch das Newtonsche Näherungsverfahren Π in der Form

$$\text{(8)} \qquad \Pi = \Pi_0(1 + \eta'\pi + \eta''\pi^2 + \cdots) \quad (\mathfrak{p}),$$

also auch umgekehrt

$$\text{(8a)} \qquad \begin{aligned} \Pi_0 &= \Pi(1 + \eta_1\pi + \eta_2\pi^2 + \cdots) \\ &= \pi^{p^f}(1 + \eta_1\pi + \cdots) \quad (\mathfrak{p}) \end{aligned}$$

darstellen kann, wo $\eta_1, \eta_2, \ldots$ wohlbestimmte $(p^f - 1)^{\text{te}}$ Einheitswurzeln bedeuten.

Daß das Newtonsche Näherungsverfahren in diesem Falle anwendbar ist, erkennt man sofort: Von den sukzessiven Ableitungen:

$$\text{(9)} \qquad \begin{aligned} \Psi'(\Pi_0) &= e_0\Pi_0^{e_0-1} + p(e_0-1)\,C_{e_0-1}\,\Pi_0^{e_0-2} + \cdots + pC_1, \\ \frac{\Psi''(\Pi_0)}{1\cdot 2} &= (e_0)_2\Pi_0^{e_0-2} + p(e_0-1)_2\,C_{e_0-1}\,\Pi_0^{e_0-3} + \cdots + pC_2 \\ &\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

ist nämlich die erste, da e_0 p nicht enthält, genau durch $\Pi_0^{e_0-1}$ teilbar, während von den späteren allgemein $\frac{\Psi^{(i)}(\Pi_0)}{i!}$ mindestens $\Pi_0^{e_0-i}$ enthält. Da endlich

$$\text{(9a)} \quad \Psi(\Pi_0) = (\Pi_0^{e_0} + pc_0^{(0)}) + pC_{e_0-1}\Pi_0^{e_0-1} + \cdots + pC_1\Pi_0 + p(C_0 - c_0^{(0)})$$

offenbar mindestens durch $p\pi$ teilbar ist, so ergeben sich in diesem Falle für die Ordnungszahlen $\varrho^{(i)}$ die Werte:

$$(10)\qquad \begin{aligned} \varrho^{(0)}+1 &\geq e_0 p^r + 1, \\ \varrho' &= (e_0-1)p^s, \\ &\vdots \\ \varrho^{(i)} &\geq (e_0 - i)p^s \\ &\vdots \end{aligned};$$

da somit allgemein: $\frac{i\varrho' - \varrho^{(i)}}{i-1} \leqq e_0 p^s$ ist, so ist ersichtlich:

$$(10a)\qquad \varrho^{(0)} + 1 > \operatorname{Max}\left(\frac{i\varrho' - \varrho^{(i)}}{i-1}\right),$$

und damit ist die Anwendbarkeit des Newtonschen Approximationsverfahrens erwiesen.

Es sei nun Π_0 eine der e_0 Wurzeln der reinen Gleichung:

$$(11)\qquad \Pi_0^{e_0} + p c_0^{(0)} = 0;$$

dann folgt aus (8), daß für $\pi^{p^s} = \Pi$ die folgende Darstellung besteht:

$$\pi^P = \Pi_0(1 + \eta'\pi + \eta''\pi^2 + \cdots + \eta^{(P-1)}\pi^{P-1} + \Pi_0\varepsilon_1),$$

wo zur Abkürzung

$$(12)\qquad p^s = P$$

gesetzt ist, und wo $\Pi_0\varepsilon_1$ genau wie in (2) a. S. 197 das Aggregat aller auf $\eta^{(P-1)}\pi^{P-1}$ folgenden Glieder bezeichnet. Schreibt man nun wieder ε_1 wie a. a. O. in derselben Form:

$$\eta_1^{(0)} + \eta_1'\pi + \cdots + \eta_1^{(P-1)}\pi^{P-1} + \Pi_0\varepsilon_2$$

und fährt so fort, so erhält man genau die a. a. O. mit (3) bezeichneten Gleichungen, in welchen nur Π_0 an die Stelle von p getreten ist; aus ihnen ergibt sich also, daß π jetzt einer Eisensteinschen Gleichung von der folgenden Form genügt:

$$\psi_0(\pi) = \pi^P + \Pi_0 c_{P-1}\pi^{P-1} + \cdots + \Pi_0 c_1 \pi + \Pi_0 c_0 = 0,$$

in welcher die Koeffizienten $c_i = \sum\limits_k \eta_k^{(i)} \Pi_0^{k-1}$ ganze p-adische Zahlen des Körpers $K(\eta, \Pi_0)$ sind, und wo c_0 eine Einheit modulo p ist.

Ist also $e = p^s e_0$ durch eine beliebig hohe Potenz von p teilbar, so genügt jede Primzahl des Bereiches $K(\alpha)$ einer Eisensteinschen Gleichung des $P = p^{s\text{-ten}}$ Grades von der Form:

$$(13)\qquad \psi_0(x) = x^P + \Pi_0 c_{P-1} x^{P-1} + \cdots + \Pi_0 c_1 x + \Pi_0 c_0 = 0,$$

in welcher Π_0 eine der e_0 Wurzeln der reinen Gleichung:

$$(13a)\qquad X^{e_0} = p\eta_0$$

und η_0 eine $(p^f - 1)^{\text{te}}$ Einheitswurzel bedeutet.

Nur diese Gleichungen des p^{ten} Grades sind jetzt also noch nach der im § 5 dargelegten Methode zu vereinfachen. Ich betrachte zunächst den einfachsten Fall, daß die Ordnungszahl e des Primteilers $\mathfrak{p}$ gleich $e_0 p$ ist, daß also die Gleichung für die algebraische Primzahl π die Form hat:

$$(14) \qquad \psi(x) = x^p + \Pi_0 c_{p-1} x^{p-1} + \cdots + \Pi_0 c_k x^k + \cdots + \Pi_0 c_0 = 0,$$

wo $\Pi_0 \sim p^{\frac{1}{e_0}} \sim \pi^p$ ist. Es sei nun $\Pi_0 c_k x^k$ das Glied des niedrigsten positiven Grades, dessen Koeffizient c_k nicht mehr durch Π_0 teilbar ist. Bildet man dann die Ableitungen

$$\psi'(\pi) = p\pi^{p-1} + \cdots + \Pi_0 c_k k \pi^{k-1} + \cdots + \Pi_0 p c_1,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$(14\text{a}) \qquad \frac{\psi^{(i)}(\pi)}{i!} = p_i \pi^{p-i} + \cdots + \Pi_0 c_k k_i \pi^{k-i} + \cdots, \qquad (i = 2, \cdots p-1)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\frac{\psi^{(p)}(\pi)}{p!} = 1,$$

so beweist man leicht die Richtigkeit der folgenden Behauptungen:

Erstens ist die Ordnungszahl von $\psi'(\pi)$

$$(15) \qquad \varrho' = p + k - 1,$$

weil das Glied $\Pi_0 c_k \cdot k\pi^{k-1}$ genau durch $\mathfrak{p}^{p+k-1}$ teilbar ist, während alle vorhergehenden Glieder eine höhere Potenz von $\mathfrak{p}$ enthalten und alle folgenden sogar mindestens durch $\Pi_0^2 \sim \mathfrak{p}^{2p}$ teilbar sind.

Zweitens ist allgemein für die Ordnungszahlen $\varrho^{(i)}$ aller Ableitungen $\frac{\psi^{(i)}(\pi)}{i!}$ bei $i = 2, 3, \cdots p-1$:

$$(15\text{a}) \qquad \varrho^{(i)} \geqq p + k - i,$$

da in dem mit $\Pi_0 \pi^{k-i}$ multiplizierten Element niedrigster Ordnung der Binomialkoeffizient k_i nur dann durch p teilbar ist, wenn er gleich Null, wenn also $i > k$ ist; ist dies aber der Fall, so tritt an die Stelle dieses Gliedes ein anderes $\Pi_0 c_{k'} \pi^{k'-i}$ von kleinster Ordnung, für welches $k' > k$ ist, während alle vorhergehenden und folgenden Glieder wieder höhere Ordnungszahlen haben.

Drittens ist für die p^{te} Ableitung offenbar:

$$(15\text{b}) \qquad \varrho^{(p)} = 0.$$

Also ist in diesem Falle

$$(15\text{c}) \qquad \begin{aligned} &\frac{i\varrho' - \varrho^{(i)}}{i-1} \leqq p + k, \qquad (i = 2, 3, \cdots p-1) \\ &\frac{p\varrho' - \varrho^{(p)}}{p-1} = \frac{p}{p-1}\varrho' = p + k + \frac{k}{p-1}. \end{aligned}$$

In diesem Falle muß also für die Ordnungszahl $\varrho^{(0)}$ des Näherungswertes die kleinste ganze Zahl gewählt werden, für welche:

(15d) $$\varrho^{(0)} + 1 > p + k + \frac{k}{p-1}\cdot$$

ist. — Ich unterscheide jetzt folgende drei Fälle:

I) $$k < p - 1 \qquad \frac{k}{p-1} < 1.$$

Dann ist jene kleinste Zahl offenbar $\varrho^{(0)} = p + k$; läßt man in $\psi(\pi)$ alle Glieder fort, deren Ordnungszahl größer ist als die von $\Pi_0\pi^k$, so ergibt sich die reduzierte Gleichung:

(16) $$\psi_0(x) = x^p + \Pi_0\eta_k x^k + \Pi_0\eta_0 = 0,$$

wo η_k und η_0 $(p^f - 1)^{te}$ Einheitswurzeln sind.

II) $k = p - 1$, dann folgt aus (15d): $\varrho^{(0)} + 1 > 2p$, also $\varrho^{(0)} = 2p$. Also wird in diesem Falle die reduzierte Gleichung:

(16a) $$\psi_0(x) = x^p + \Pi_0\eta_{p-1}x^{p-1} + \Pi_0(\eta_0 + \Pi_0\eta_0') = 0.$$

III) $k = p$, dann muß $\varrho^{(0)} + 1 > 2p + 1 + \frac{1}{p-1}$, also $\varrho^{(0)} = 2p + 1$ sein. Also wird jetzt

(16b) $$\psi_0(x) = x^p + \Pi_0^2\eta_1 x + \Pi_0(\eta_0 + \Pi_0\eta_0') = 0.$$

In allen Fällen wird also π hier durch eine sehr einfache trinomische Gleichung definiert.

Ich betrachte jetzt den allgemeinsten Fall, daß:

(17) $$e = p^s e_0$$

durch die s^{te} Potenz von p genau teilbar ist. Dann genügt also π der Eisensteinschen Gleichung des e^{ten} Grades:

(18) $$\psi(x) = \pi^e + pc_{e-1}\pi^{e-1} + pc_{e-2}\pi^{e-2} + \cdots + pc_0 = 0,$$

welche wir durch eine reine Gleichung des e_0^{ten} Grades und eine neue Eisensteinsche Gleichung des $\frac{e}{e_0} = (p^s)^{ten}$ Grades ersetzen könnten. Da aber die nun anzugebende Reduktion unabhängig von dem Grade der zu reduzierenden Gleichung ist, so will ich gleich für die vorliegende Gleichung (18) untersuchen, von welcher Ordnung $\varrho^{(0)}$ die Näherungsgleichung $\psi_0(x) = 0$ gewählt werden muß, damit die Primzahl π durch die ihr äquivalente Wurzel π_0 jener Näherungsgleichung ersetzt werden kann.

In diesem allgemeinsten Falle ist nun die Ordnungszahl von:

$$(18\text{a})\qquad \psi'(\pi) = e\pi^{e-1} + p(e-1)\,c_{e-1}\pi^{e-2} + \cdots + pc_1$$

höchstens gleich der des Anfangsgliedes $e\pi^{e-1}$, da dieses sicher in $\psi'(\pi)$ auftritt und sich nicht fortheben kann, d. h. es ist:

$$(19)\qquad \varrho' \leqq se + e - 1,$$

während für alle folgenden Ordnungszahlen:

$$(19\text{a})\qquad \varrho^{(i)} \geqq e - i$$

ist, da in jeder Ableitung: $\frac{\psi^{(i)}(\pi)}{i!} = e_i\pi^{e-i} + \cdots$ das Anfangsglied mindestens durch $\mathfrak{p}^{e-i}$, alle folgenden aber mindestens durch $p \sim \mathfrak{p}^e$ teilbar sind. Also ist in diesem Falle:

$$(19\text{b})\qquad \frac{i\varrho' - \varrho^{(i)}}{i-1} \leqq \frac{i(se+e-1)-(e-i)}{i-1} = e\left(\frac{i}{i-1}s + 1\right)$$
$$\leqq e(2s+1).$$

Wählt man also hier:

$$(20)\qquad \varrho^{(0)} \geqq e(2s+1),$$

so geschieht der Bedingung (10a) für $\varrho^{(0)}$ sicher Genüge. Man erhält sicher die $\varrho^{(0)\text{te}}$ Näherungsfunktion $\psi_0(x)$, wenn man in den Koeffizienten pc_i von $\psi(x)$ alle Glieder fortläßt, welche mit p^{2s+1} multipliziert sind. Es ergibt sich also in diesem allgemeinsten Falle der Satz:

> Ist die Ordnungszahl $e = p^s e_0$ des Primteilers $\mathfrak{p}$ durch p teilbar, so kann man eine zu $\mathfrak{p}$ gehörige Primzahl π innerhalb des Körpers $K(\alpha)$ stets so auswählen, daß sie durch eine Gleichung:
>
> $$\psi_0(x) = x^e + pc_{e-1}x^{e-1} + \cdots + pc_1x + pc_0 = 0$$
>
> definiert sind, deren Koeffizienten
>
> $$c_i = \eta_0^{(i)} + \eta_1^{(i)}p + \cdots + \eta_{2s}^{(i)}p^{2s}$$
>
> solche ganze Zahlen des Koeffizientenkörpers $K(\eta)$ sind, daß ihre Entwickelung nach Potenzen von p höchstens bis zum $2s^{\text{ten}}$ Grade ansteigt.

Ich bemerke noch, daß in dem allgemeinsten Falle, wo $e = e_0p^s$ ist, die Gleichung für π nicht bloß durch zwei Gleichungen vom e_0^{ten} und vom $(p^s)^{\text{ten}}$ Grade, sondern durch eine völlig bestimmte Kette von mehreren einfachen Gleichungen ersetzt werden kann, und daß gerade diese Zerlegung jener Gleichungen einen sehr wichtigen Einblick in die algebraische Natur des betrachteten Körpers gewährt. Doch soll hierauf erst an einer späteren Stelle genauer eingegangen werden.

§ 7. Der zu einem Primteiler $\mathfrak{p}$ gehörige Wurzelzyklus.

Mit Hilfe der bis jetzt gefundenen Resultate untersuche ich nun das Verhalten der Zahlen eines algebraischen Körpers $K(\alpha)$ in bezug auf einen beliebigen Primdivisor $\mathfrak{p}$. Es sei e die Ordnung und f der Grad von $\mathfrak{p}$, und es werde wieder $\lambda = ef$ gesetzt. Ist dann $\beta = \varphi(\alpha)$ irgend eine Zahl des Körpers $K(\alpha)$, so genügt diese für den Bereich von $\mathfrak{p}$ einer Gleichung λ^{ten} Grades.

(1) $$G(y) = 0, \quad (\mathfrak{p})$$

mit rationalen p-adischen Koeffizienten, deren linke Seite im allgemeinen irreduktibel ist, und falls sie reduktibel sein sollte, einer Potenz einer irreduktiblen Funktion gleich ist. Es sei speziell β eine eigentliche Zahl von $K(\alpha)$, dann ist jene Gleichung irreduktibel.

Ist β_1 eine der λ zu $\mathfrak{p}$ gehörigen algebraischen p-adischen Zahlen, denen β gleich ist, so besteht für diese eine Darstellung von der folgenden Form:

(2) $$\beta_1^{(0)} = \eta_0 + \eta_1 \pi_1^{(0)} + \eta_2 \pi_1^{(0)^2} + \cdots \quad (\mathfrak{p}),$$

wo $\pi_1^{(0)} \sim p^{\frac{1}{e}}$ eine zu $\mathfrak{p}$ gehörige Primzahl von $K(\alpha_1)$ ist, und die Koeffizienten η_i eindeutig bestimmte $(p^f - 1)^{\text{te}}$ Einheitswurzeln bedeuten. Die Primzahl $\pi_1^{(0)}$ genügt nebst ihren e konjugierten:

(3) $$\pi_1^{(0)}, \pi_2^{(0)}, \cdots \pi_e^{(0)}$$

einer im vorigen Abschnitte näher bestimmten reduzierten Eisensteinschen Gleichung:

(4) $$\psi(x, \eta) = x^e + p c_{e-1}^{(0)} x^{e-1} + \cdots + p c_0^{(0)} = 0,$$

deren Koeffizienten $c_i^{(0)}$ ganze Zahlen des Koeffizientenkörpers f^{ten} Grades $K(\eta)$ sind, und diese Gleichung ist innerhalb jenes Körpers $K(\eta)$ irreduktibel. Daraus folgt wörtlich ebenso, wie bei dem Satze (5) a. S. 131, daß jede Gleichung für $\pi_1^{(0)}$ mit rationalen p-adischen Koeffizienten oder aber auch mit p-adischen Koeffizienten des Körpers $K(\eta)$ richtig bleibt, wenn $\pi_1^{(0)}$ durch die konjugierten Zahlen (3) ersetzt wird. Da nun die Gleichung (1) die eine Wurzel $y = \beta_1^{(0)}$ hat, so ist $G(\beta_1^{(0)}) = 0$, und diese Gleichung bleibt richtig, wenn $\beta_1^{(0)}$ durch die e konjugierten Zahlen

(5) $$\begin{aligned} \beta_1^{(0)} &= \eta_0 + \eta_1 \pi_1^{(0)} + \eta_2 \pi_1^{(0)^2} + \cdots \\ \beta_2^{(0)} &= \eta_0 + \eta_1 \pi_2^{(0)} + \eta_2 \pi_2^{(0)^2} + \cdots \\ &\vdots \\ \beta_e^{(0)} &= \eta_0 + \eta_1 \pi_e^{(0)} + \eta_2 \pi_e^{(0)^2} + \cdots \end{aligned} \quad (\mathfrak{p})$$

ersetzt wird. Da ferner jede symmetrische Funktion

$$S(\beta_1^{(0)}, \beta_2^{(0)}, \cdots \beta_e^{(0)})$$

dieser e konjugierten Zahlen auch eine symmetrische Funktion von $(\pi_1^{(0)}, \cdots \pi_e^{(0)})$, also eine p-adische Zahl des Koeffizientenkörpers $K(\eta)$ ist, so genügt die Zahl $\beta_1^{(0)}$ nebst ihren konjugierten $\beta_2^{(0)}, \cdots \beta_e^{(0)}$ einer Gleichung e^{ten} Grades:

$$(6) \qquad g(y,\eta) = (y - \beta_1^{(0)})(y - \beta_2^{(0)}) \cdots (y - \beta_e^{(0)})$$

mit p-adischen Koeffizienten des Koeffizientenkörpers $K(\eta)$, deren linke Seite ein Teiler der rationalen p-adischen Funktion ef^{ten} Grades $G(y)$ in (1) ist.

Die so sich ergebende Gleichung:

$$(7) \qquad G(y) = g(y, \eta)\, \overline{G}\,(y, \eta)$$

bleibt nun nach dem a. S. 192 unten bewiesenen Satze richtig, wenn man in ihr die Einheitswurzel η durch ihre f modulo $\mathfrak{p}$ konjugierten $\eta, \eta^p, \eta^{p^2}, \cdots \eta^{p^{f-1}}$ ersetzt, und aus den so sich ergebenden f Gleichungen:

$$(7\,\text{a}) \qquad G(y) = g\left(y, \eta^{p^k}\right) \overline{G}\left(y, \eta^{p^k}\right) \qquad (k = 0, 1, \cdots f-1)$$

folgt, daß $G(y)$ auch durch jede der f konjugierten Funktionen e^{ten} Grades:

$$g(y, \eta),\ g(y, \eta^p),\ \cdots\ g(y, \eta^{p^{f-1}})$$

teilbar sein muß. Nun ist endlich das Produkt jener f Funktionen:

$$\overline{G}\,(y) = g(y, \eta) \cdot g(y, \eta^p) \cdots g(y, \eta^{p^{f-1}})$$

als symmetrische Funktion der f konjugierten Zahlen η^{p^k} eine ganze Funktion des $\lambda = ef^{\text{ten}}$ Grades von y mit rationalen p-adischen Koeffizienten, und diese hat mit der irreduktiblen Funktion λ^{ten} Grades $G(y)$ den Teiler $g(y, \eta)$ gemeinsam; also muß $G(y) = \overline{G}(y)$ sein, wenn man noch hinzunimmt, daß in beiden Funktionen die Koeffizienten von y^λ gleich Eins sind. Es besteht somit die Gleichung:

$$(8) \qquad G(y) = g(y, \eta) \cdot g(y, \eta^p) \cdots g(y, \eta^{p^{f-1}}),$$

d. h. die λ konjugierten p-adischen Zahlen $\beta_1, \beta_2, \cdots \beta_\lambda$ sind identisch mit den Wurzeln der f Gleichungen e^{ten} Grades:

$$(9) \qquad g(y, \eta^{p^k}) = 0 \qquad (k = 0, 1, \cdots f-1).$$

Alle diese ef Wurzeln sind voneinander verschieden, weil dasselbe von den ihnen gleichen Zahlen $\beta_1, \cdots \beta_\lambda$ gilt. Hieraus folgt leicht, daß die f Gleichungen e^{ten} Grades (9) innerhalb des Koeffizientenkörpers $K(\eta)$ irreduktibel sind. Diese Tatsache braucht nur für eine dieser f Gleichungen, etwa für die erste bewiesen zu werden; denn zerfiele z. B. die letzte in zwei Faktoren niedrigeren Grades, so würde aus der Gleichung:

$$g(y, \eta^{p^{f-1}}) = g_1(y, \eta)\; g_2(y, \eta)$$

durch die erlaubte Verwandlung von η in η^p

$$g(y, \eta) = g_1(y, \eta^p)\; g_2(y, \eta^p)$$

folgen, $g(y, \eta)$ wäre also ebenfalls zerlegbar.

Angenommen nun, $g(y, \eta)$ sei zerlegbar und

$$g(y, \eta) = h(y, \eta) \cdot k(y, \eta)$$

sei eine Zerlegung dieser Funktion in zwei Faktoren niedrigeren Grades; ist dann $\beta_1^{(0)}$ eine Wurzel der Gleichung $h(y, \eta) = 0$, so muß die Gleichung $h(\beta_1^{(0)}, \eta) = 0$ richtig bleiben, wenn man $\beta_1^{(0)}$ durch die e konjugierten Wurzeln $\beta_2^{(0)}, \cdots \beta_e^{(0)}$ ersetzt, und da diese alle voneinander verschieden sind, so ist die Annahme, daß $g(y, \eta)$ einen Teiler niedrigeren Grades besitzt, falsch. Es ergibt sich also zunächst der Satz:

> Die irreduktible Funktion λ^{ten} Grades $G(y)$ mit rationalen p-adischen Koeffizienten, der eine beliebige Zahl β des Körpers $K(\alpha)$ für den Bereich eines Primteilers $\mathfrak{p}$ von p genügt, zerfällt unter Adjunktion des Koeffizientenkörpers $K(\eta)$ in f irreduktible konjugierte Faktoren e^{ten} Grades.

Es seien nun allgemein:

$$\beta_1^{(k)},\; \beta_2^{(k)}, \cdots \beta_e^{(k)}$$

die e Wurzeln der irreduktiblen Gleichung

$$g(y, \eta^{p^k}) = (y - \beta_1^{(k)})\,(y - \beta_2^{(k)}) \cdots (y - \beta_e^{(k)}) = 0.$$

Da sich die linke Seite dieser Gleichung aus

$$g(y, \eta) = (y - \beta_1^{(0)})\,(y - \beta_2^{(0)}) \cdots (y - \beta_e^{(0)})$$

durch die Verwandlung von η in η^{p^k} ergibt, so gehen ihre Wurzeln aus den Reihen $\beta_i^{(0)}$ durch dieselbe Substitution hervor. Macht man

diese Substitution bei den Wurzeln $\beta_1^{(0)}, \cdots \beta_e^{(0)}$ in (5), so erhält man für den zu $g(y, \eta^{p^k})$ gehörigen Unterzyklus die folgende Darstellung:

$$
\begin{aligned}
&\beta_1^{(k)} = \eta_0^{p^k} + \eta_1^{p^k}\pi_1^{(k)} + \eta_2^{p^k}\pi_1^{(k)^2} + \cdots \\
(10)\qquad &\beta_2^{(k)} = \eta_0^{p^k} + \eta_1^{p^k}\pi_2^{(k)} + \eta_2^{p^k}\pi_2^{(k)^2} + \cdots \qquad (\mathfrak{p}) \\
&\vdots \\
&\beta_e^{(k)} = \eta_0^{p^k} + \eta_1^{p^k}\pi_e^{(k)} + \eta_2^{p^k}\pi_e^{(k)^2} + \cdots,
\end{aligned}
$$

und hier sind die zugehörigen Primzahlen $\pi_1^{(k)}, \pi_2^{(k)}, \cdots \pi_e^{(k)}$ die e konjugierten Wurzeln der Gleichung:

$$(11)\qquad \psi(x, \eta^{p^k}) = x^e + pc_{e-1}^{(k)}x^{e-1} + \cdots + pc_0^{(k)} = 0,$$

deren linke Seite aus (4) dadurch hervorgeht, daß η durch η^{p^k} ersetzt wird. Es ergibt sich also der folgende Satz:

Ist $\mathfrak{p}$ ein Primteiler einer reellen Primzahl p für den Körper $K(\alpha)$, dessen Ordnung e und dessen Grad f ist, und β eine Zahl dieses Körpers, so zerfällt der ef-gliedrige Zyklus der zu $\mathfrak{p}$ gehörigen konjugierten p-adischen algebraischen Zahlen unter Adjunktion des Koeffizientenkörpers $K(\eta)$ in f Unterzyklen:

$$
\begin{aligned}
&\beta_1^{(0)},\quad \beta_2^{(0)},\quad \cdots \beta_e^{(0)} \\
(12)\qquad &\beta_1^{(1)},\quad \beta_2^{(1)},\quad \cdots \beta_e^{(1)} \\
&\vdots \\
&\beta_1^{(f-1)}, \beta_2^{(f-1)}, \cdots \beta_e^{(f-1)}
\end{aligned}
$$

von je e für den Bereich von $K(\eta)$ konjugierten p-adischen Zahlen. Die e Zahlen $\beta_1^{(k)}, \cdots \beta_e^{(k)}$ eines solchen Unterzyklus gehen aus der ersten $\beta_1^{(k)}$ dadurch hervor, daß die Entwicklungszahl $\pi_1^{(k)}$ durch ihre für den Bereich von $K(\eta)$ konjugierten $\pi_2^{(k)}, \cdots \pi_e^{(k)}$ ersetzt wird, und die Zahlen aller f Unterzyklen ergeben sich aus den entsprechenden des ersten Zyklus dadurch, daß für η der Reihe nach die konjugierten Zahlen $\eta^p, \eta^{p^2}, \cdots \eta^{p^{f-1}}$ substituiert werden.

Die Entwicklungen (10) der e Wurzeln $(\beta_1^{(k)}, \beta_2^{(k)}, \cdots \beta_e^{(k)})$ gehen dadurch aus den entsprechenden Reihen (5) für $(\beta_1^{(0)}, \beta_2^{(0)}, \cdots \beta_e^{(0)})$ hervor, daß in den letzteren die Koeffizienten $\eta_0, \eta_1, \eta_2, \cdots$ durch ihre $(p^k)^{\text{ten}}$ Potenzen ersetzt und zugleich die Wurzeln $(\pi_1^{(0)}, \cdots \pi_e^{(0)})$ der Gleichung $\psi(x, \eta) = 0$ in (4) durch die Wurzeln $(\pi_1^{(k)}, \cdots \pi_e^{(k)})$ derjenigen Gleichung $\psi(x, \eta^{p^k}) = 0$ in (11) ersetzt werden, deren linke

Seite aus der vorigen durch dieselbe Vertauschung der Einheiten η mit ihren $(p^k)^{\text{ten}}$ Potenzen hervorgeht. Aus diesem Grunde will ich in konsequenter Erweiterung der a. S. 195 oben eingeführten Bezeichnung die ef konjugierten p-adischen Reihen (12) auch mitunter durch:

$$
\text{(12a)} \qquad
\begin{array}{llll}
\beta_1, & \beta_2, & \cdots & \beta_e, \\
\beta_1^{(p)}, & \beta_2^{(p)}, & \cdots & \beta_e^{(p)}, \\
\vdots & & & \\
\beta_1^{(p^{f-1})}, & \beta_2^{(p^{f-1})}, & \cdots & \beta_e^{(p^{f-1})}
\end{array}
$$

bezeichnen.

Neuntes Kapitel.

Die Darstellung der ganzen algebraischen Zahlen durch ein Fundamentalsystem und die Bestimmung der Körperdiskriminante. Das zu einem Divisor gehörige Ideal.

---

§ 1. Vereinfachung der Aufgabe.

Ich wende mich jetzt zu einer genaueren Untersuchung der ganzen algebraischen Zahlen eines Körpers $K(\alpha)$, insbesondere zu ihrer Darstellung durch ein Fundamentalsystem, um dann die Eigenschaften dieser Fundamentalsysteme und die Zusammensetzung der zugehörigen Körperdiskriminanten darzulegen.

Da eine algebraische Zahl des Körpers $K(\alpha)$ dann und nur dann algebraisch ganz ist, wenn sie in bezug auf jeden Primteiler $\mathfrak{p}$ dieses Körpers ganz ist, so reduziert sich die vorliegende Aufgabe auf die einfachere, alle für den Bereich eines Primfaktors $\mathfrak{p}$ ganzen algebraischen Zahlen von $K(\alpha)$ durch ein Fundamentalsystem modulo $\mathfrak{p}$ darzustellen.

Es sei wieder $\mathfrak{p}$ ein zu der reellen Primzahl p gehöriger Primteiler von der Ordnung e und vom Grade f, und es sei $ef = \lambda$. Ist dann β eine beliebige Zahl des Körpers $K(\alpha)$, und sind: $\beta_1, \beta_2, \ldots \beta_\lambda$ die λ zu $\mathfrak{p}$ gehörigen konjugierten p-adischen algebraischen Zahlen, so genügen diese stets einer algebraischen Gleichung λ^{ten} Grades mit rationalen p-adischen Koeffizienten, deren linke Seite entweder selbst irreduktibel oder die Potenz einer irreduktiblen Funktion ist. Nach dem a. S. 132 bewiesenen Satze kann man dann stets ein solches System von λ ganzen algebraischen Zahlen

(1) $$\eta^{(1)}, \eta^{(2)}, \ldots \eta^{(\lambda)}$$

des Körpers $K(\alpha)$ bestimmen, daß jede andere ganze Zahl γ auf eine einzige Weise in der Form:

(1a) $$\gamma = u_1\eta^{(1)} + u_2\eta^{(2)} + \cdots + u_\lambda\eta^{(\lambda)}$$

mit ganzen rationalen p-adischen Koeffizienten darstellbar ist. Ein solches System werde ein Fundamentalsystem für den Bereich

von $\mathfrak{p}$ genannt. Ein System von λ ganzen algebraischen Zahlen ist dann und nur dann ein solches Fundamentalsystem für den Bereich von $\mathfrak{p}$, wenn die aus seinen Konjugierten gebildete Diskriminante:

$$D(\eta^{(1)}, \eta^{(2)}, \cdots \eta^{(\lambda)}) = \begin{vmatrix} \eta_1^{(1)}, \eta_1^{(2)}, \dots \eta_1^{(\lambda)} \\ \eta_2^{(1)}, \eta_2^{(2)}, \dots \eta_2^{(\lambda)} \\ \vdots \\ \eta_\lambda^{(1)}, \eta_\lambda^{(2)}, \dots \eta_\lambda^{(\lambda)} \end{vmatrix}^2$$

durch eine möglichst niedrige Potenz von p teilbar ist. Die in $D(\eta^{(1)}, \eta^{(2)}, \dots \eta^{(\lambda)})$ enthaltene Potenz von p soll der zu $\mathfrak{p}$ gehörige Diskriminantenteiler des Körpers $K(\alpha)$ genannt und, vorbehaltlich einer später anzugebenden kleinen Änderung, durch $D(\mathfrak{p})$ bezeichnet werden. Zu einem jeden Primteiler $\mathfrak{p}$ gehört ein solcher Diskriminantenteiler. Es wird sich nun zeigen, daß die Körperdiskriminante, deren Bestimmung die Hauptaufgabe dieses Kapitels ist, abgesehen vom Vorzeichen gleich dem Produkte $\Pi D(\mathfrak{p})$ der zu allen Primfaktoren $\mathfrak{p}$ gehörigen Diskriminantenteiler ist. Aus diesem Grunde soll in den beiden nächsten Paragraphen zu einem Primdivisor $\mathfrak{p}$ ein Fundamentalsystem (1) bestimmt, und aus ihm der zu $\mathfrak{p}$ gehörige Diskriminantenteiler $D(\mathfrak{p})$ gefunden werden

§ 2. Bestimmung des Diskriminantenteilers $D(\mathfrak{p})$, wenn der Grad f oder wenn die Ordnung e des Primteilers $\mathfrak{p}$ gleich Eins ist.

Ich betrachte zuerst den einfachsten Fall, daß der Primteiler $\mathfrak{p}$ kein Verzweigungsteiler, daß also seine Ordnung $e = 1$, mithin $\lambda = f$ ist. In diesem Falle ist also p selbst für den Bereich von $\mathfrak{p}$ eine Primzahl, und die f für den Bereich von $\mathfrak{p}$ zu einer Zahl β konjugierten p-adischen algebraischen Zahlen

$$(1)\qquad \begin{aligned} \beta_1 &= \eta_0 + \eta_1 p + \eta_2 p^2 + \cdots, \\ \beta_2 &= \eta_0^p + \eta_1^p p + \eta_2^p p^2 + \cdots, \\ &\vdots \\ \beta_f &= \eta_0^{p^{f-1}} + \eta_1^{p^{f-1}} p + \eta_2^{p^{f-1}} p^2 + \cdots \end{aligned}$$

schreiten nach ganzen Potenzen von p fort mit Koeffizienten, welche konjugierte $(p^f - 1)^{\text{te}}$ Einheitswurzeln sind.

Ist nun η eine primitive $(p^f - 1)^{\text{te}}$ Einheitswurzel, deren f konjugierte $\eta, \eta^p, \eta^{p^2}, \dots \eta^{p^{f-1}}$ also alle voneinander verschieden, mithin auch modulo p inkongruent sind, so bilden die f Potenzen $(1, \eta, \eta^2, \dots \eta^{f-1})$ ein Fundamentalsystem modulo $\mathfrak{p}$; denn ihre Diskriminante:

der Einheit oder Null, und $\pi_1, \pi_2, \ldots \pi_e$ sind die e konjugierten Wurzeln einer bestimmten reduzierten Gleichung:

$$\psi(x) = x^e + pc_{e-1}x^{e-1} + \cdots + pc_0 = 0 \tag{3}$$

mit rationalen ganzzahligen Koeffizienten c_i. In diesem Falle beweist man leicht die Richtigkeit des folgenden wichtigen Satzes:

Ist $\mathfrak{p}$ ein Primteiler von $K(\alpha)$ vom Grade Eins und $\pi \sim p^{\frac{1}{e}}$ eine zu $\mathfrak{p}$ gehörige Primzahl von $K(\alpha)$, so bilden die e ganzen algebraischen Zahlen

$$1,\ \pi,\ \pi^2,\ \ldots\ \pi^{e-1} \tag{4}$$

ein Fundamentalsystem modulo $\mathfrak{p}$ für $K(\alpha)$, d. h. jede modulo $\mathfrak{p}$ ganze algebraische Zahl β dieses Körpers ist auf eine einzige Weise in der Form:

$$\beta = u_0 + u_1\pi + u_2\pi^2 + \cdots + u_{e-1}\pi^{e-1} \tag{4a}$$

mit ganzen rationalen p-adischen Koeffizienten u_i darstellbar.

Da π die Wurzel der für den Bereich von p irreduktiblen Gleichung e^{ten} Grades (3) ist, so ist zunächst jede ganze oder gebrochene Zahl β auf eine einzige Weise in der Form (4a) mit rationalen p-adischen Koeffizienten u_i darstellbar; es ist also nur noch zu zeigen, daß diese Koeffizienten dann und nur dann ganz sind, wenn β algebraisch ganz, also durch eine nicht negative Potenz von $\mathfrak{p}$ teilbar ist. Dies erkennt man aber sehr leicht. Sei nämlich für eine bestimmte Zahl β etwa $u_i\pi^i$ derjenige unter den e Summanden von β, dessen Ordnungszahl ϱ_i die kleinste ist. Dann besitzt auch β dieselbe Ordnungszahl; denn da die e Produkte $u_k\pi^k$ ebenso, wie a. S. 199 in (7b), verschiedene Ordnungszahlen besitzen, so kann sich das Anfangsglied von $u_i\pi^i$ nicht gegen ein anderes fortheben. Also ist β dann und nur dann modulo $\mathfrak{p}$ algebraisch ganz, wenn die Ordnungszahl ϱ_i dieses Gliedes $u_i\pi^i$ Null oder positiv ist, und dies ist nur dann der Fall, wenn der Koeffizient u_i in bezug auf p von nicht negativer Ordnung ist. Denn wenn $u_i = \frac{v_i}{p}$ auch nur durch die erste Potenz von p teilbar wäre, so besäße ja das Produkt

$$u_i\pi^i = \frac{v_i\pi^i}{p} \sim \frac{v_i}{\pi^{e-i}}$$

sicher eine negative Ordnungszahl. Ebenso folgt nun, daß auch alle Koeffizienten u_k der anderen Potenzen von π in (4a) ganze p-adische

Zahlen sein müssen, und damit ist unsere Behauptung vollständig bewiesen.

Ich stelle nun auch hier die Frage, wie groß der zugehörige Diskriminantenteiler $D(\mathfrak{p})$ ist, d. h. durch welche Potenz von p die Diskriminante:

$$(5) \qquad D(\pi) = \begin{vmatrix} 1, & \pi_1, & \pi_1^2, & \dots & \pi_1^{e-1} \\ 1, & \pi_2, & \pi_2^2, & \dots & \pi_2^{e-1} \\ \vdots & & & & \\ 1, & \pi_e, & \pi_e^2, & \dots & \pi_e^{e-1} \end{vmatrix}^2 = \pm \prod_{i \gtrless k} (\pi_i - \pi_k)$$

des Fundamentalsystems (4) genau teilbar ist. Da jede der $e(e-1)$ Differenzen $(\pi_i - \pi_k)$ mindestens durch die erste Potenz von $\mathfrak{p}$ teilbar ist, so enthält $D(\pi)$ mindestens die Potenz

$$(5a) \qquad \mathfrak{p}^{e(e-1)} \sim p^{e-1},$$

und man zeigt leicht, daß dies, falls e nicht durch p teilbar ist, auch die höchste in $D(\pi)$ enthaltene Potenz von p ist.

In der Tat ist nach (7b) und (6a) a. S. 105

$$(6) \qquad D(\pi) = (-1)^{\frac{e(e-1)}{2}} n_{\mathfrak{p}}(\psi'(\pi_1)).$$

Ist nun e durch p nicht teilbar, so kann man $\psi(x)$ in der reduzierten Form annehmen:

$$(7) \qquad \psi(x) = x^e - \omega p,$$

wo ω eine bestimmte $(p-1)^{\text{te}}$ Wurzel der Einheit bedeutet. Also ist:

$$n_{\mathfrak{p}}(\psi'(\pi_1)) = n_{\mathfrak{p}}(e\pi_1^{e-1}) = e^e(n(\pi_1))^{e-1},$$

und da aus der Gleichung (7) für π_1

$$n(\pi_1) = (-1)^{e-1} \omega p$$

folgt, so ergibt sich schließlich leicht:

$$(8) \qquad D(\pi) = (-1)^{\frac{(e-1)(e-2)}{2}} e^e \omega^{e-1} p^{e-1},$$

also

$$D(\mathfrak{p}) = p^{e-1},$$

und damit ist unsere Behauptung vollständig bewiesen.

Die in (6) gefundene Gleichung:

$$D(\pi) = (-1)^{\frac{e(e-1)}{2}} n_{\mathfrak{p}}(\psi'(\pi_1))$$

ergibt aber auch, falls e durch eine Potenz von p teilbar ist, die vollständige Bestimmung der Körperdiskriminante. Zu diesem Zwecke bilde ich die Ableitung:

$$\psi'(\pi_1) = e\pi_1^{e-1} + p(e-1)\,c_{e-1}\,\pi_1^{e-2} + \cdots p i c_i \pi_1^{i-1} + \cdots + p c_1 \tag{9}$$

und entwickele sie nach steigenden Potenzen von π_1. Da die e einzelnen Glieder von $\psi'(\pi_1)$ wieder alle von verschiedener Ordnung in Bezug auf $\mathfrak{p}$ sind, so können sich keine Glieder niedrigster Ordnung fortheben. Setzt man also:

$$\psi'(\pi_1) = c_{\bar{e}-1}\,\pi_1^{\bar{e}-1} + c_{\bar{e}}\,\pi_1^{\bar{e}} + \cdots, \tag{9a}$$

so ist das Anfangsglied von $\psi'(\pi_1)$ einfach das Anfangsglied des Summanden niedrigster Ordnung:

$$p\,i\,c_i\,\pi_1^{i-1}$$

in $\psi'(\pi_1)$, welches in jedem Falle unmittelbar angegeben werden kann. Bildet man nun die Norm von $\psi'(\pi_1)$ und beachtet dabei, daß

$$n_{\mathfrak{p}}(\pi_1) = (-1)^e p c_0$$

ist, so erhält man für $D(\pi)$ und somit für $D(\mathfrak{p})$ die Werte:

$$D(\pi) = (-1)^{\frac{e(e-1)}{2}}\, c_{\bar{e}-1}^{e}\,((-1)^e p\, c_0)^{\bar{e}-1} + \cdots,$$

$$D(\mathfrak{p}) = \mathfrak{p}^{\bar{e}-1}. \tag{10}$$

Die Zahl $\bar{e}$, d. h. die um Eins vermehrte Ordnungszahl von $\psi'(\pi)$ soll die **Verzweigungsordnung des Divisors** $\mathfrak{p}$ genannt werden. Im allgemeinen ist $\bar{e}$ gleich der Ordnung e des Primteilers $\mathfrak{p}$; dies ist nämlich stets und nur dann der Fall, wenn e durch p nicht teilbar ist. Dann ist nämlich $\psi'(\pi_1) = e\pi_1^{e-1}$ also genau durch $\mathfrak{p}^{e-1}$ teilbar. Enthält dagegen $e = p^s e_0$ eine Potenz von p als Teiler, so ist $\bar{e} > e$ und zwar zeigt man leicht, daß die ganze Zahl $\bar{e}$ stets zwischen den beiden Grenzen:

$$e + 1 \quad \text{und} \quad (s+1)e$$

liegen muß. In der Tat ergibt sich ja der größte Wert, den die Verzweigungsordnung $\bar{e}$ annehmen kann, wenn in $\psi'(\pi_1)$ das Anfangsglied $e\pi_1^{e-1} = p^s e_0 \pi_1^{e-1}$ das Glied niedrigster Ordnung ist; alsdann ist:

$$\bar{e} = (s+1)e.$$

Der kleinste Wert wird erhalten, wenn in dem Endglied pc_1 von $\psi'(\pi_1)$ der Koeffizient c_1 eine Einheit ist. Dann ist wirklich $\bar{e} - 1 = e$ also $\bar{e} = e + 1$. So ergibt sich also hier das Schlußresultat:

Ist $\mathfrak{p}$ ein Primteiler von $K(\alpha)$ vom Grade Eins und von der Ordnung e, so ist der zu $\mathfrak{p}$ gehörige Diskriminantenteiler $D(\mathfrak{p})$ stets gleich $\mathfrak{p}^{\bar{e}-1}$, wenn $\bar{e}$ die Verzweigungsordnung von $\mathfrak{p}$ bedeutet. Die Verzweigungsordnung $\bar{e}$ ist stets und nur dann gleich der Ordnung e von $\mathfrak{p}$, wenn e durch p nicht teilbar ist. Ist dagegen $e = p^s e_0$, so ist $\bar{e}$ eine zwischen den beiden Grenzen $e+1$ und $(s+1)e$ liegende ganze Zahl, welche aus der Gleichung für π in jedem Falle leicht bestimmt werden kann.

§ 3. Bestimmung des Diskriminantenteilers $D(\mathfrak{p})$ für einen beliebigen Primdivisor $\mathfrak{p}$.

Ich untersuche nun den allgemeinsten Fall, daß die Ordnung e und der Grad f von $\mathfrak{p}$ beliebige ganze Zahlen sind. Dann genügt jede Zahl des Körpers $K(\alpha)$ für den Bereich von $\mathfrak{p}$ einer Gleichung des e^{ten} Grades

(1) $$g(x, \eta) = 0 \qquad (\mathfrak{p}),$$

deren Koeffizienten p-adische Zahlen des Koeffizientenkörpers $K(\eta)$ sind. Man kann also zunächst genau nach der a. S. 111 flgde. dargelegten Methode ein Fundamentalsystem für den Bereich von $\mathfrak{p}$ in bezug auf $K(\eta)$, d. h. ein System von e ganzen Zahlen von $K(\alpha)$

(2) $$\xi^{(1)}, \xi^{(2)}, \ldots \xi^{(e)}$$

so auswählen, daß alle modulo $\mathfrak{p}$ ganzen Zahlen dieses Körpers auf eine einzige Weise in der Form:

(2a) $$U_1 \xi^{(1)} + U_2 \xi^{(2)} + \cdots + U_e \xi^{(e)}$$

mit ganzen Koeffizienten von $K(\eta)$ darstellbar ist. Auch hier findet man leicht ein derartiges System; ist nämlich π eine Primzahl modulo $\mathfrak{p}$, so ist wieder:

(2b) $$1, \pi, \pi^2, \cdots \pi^{e-1}$$

ein solches Fundamentalsystem. Da nämlich π innerhalb $K(\eta)$ einer irreduktiblen Gleichung des e^{ten} Grades genügt, so ist jede ganze oder gebrochene Zahl β von $K(\alpha)$ auf eine einzige Weise in der Form:

(2c) $$\beta = U_0 + U_1 \pi + \cdots + U_{e-1} \pi^{e-1}$$

mit ganzen oder gebrochenen p-adischen Koeffizienten von $K(\eta)$ darstellbar, und da auch hier alle e Produkte $U_i \pi^i$ verschiedene Ord-

nungszahlen haben, so ist die Ordnungszahl von β wieder gleich der niedrigsten Ordnung jener e Produkte. Soll also β algebraisch ganz sein, so darf keins dieser Produkte eine negative Ordnungszahl haben, d. h. β ist dann und nur dann algebraisch ganz, wenn alle Koeffizienten U_i ganze p-adische Zahlen von $K(\eta)$ sind; das System (2b) ist somit wirklich ein Fundamentalsystem in bezug auf den Koeffizientenkörper $K(\eta)$.

Es sei nun:

$$\begin{aligned}\psi(x, \eta) &= x^e + p\,c_{e-1}^{(0)} x^{e-1} + \cdots + p\,c_0^{(0)} \\ &= (x - \pi_1^{(0)})(x - \pi_2^{(0)}) \cdots (x - \pi_e^{(0)}) \quad (\mathfrak{p})\end{aligned} \tag{3}$$

die Gleichung, der $\pi = \pi_1^{(0)}$ nebst seinen konjugierten genügt. Dann ist wieder die Diskriminante

$$D(\pi^{(0)}) = \left| 1, \pi_i^{(0)}, \pi_i^{(0)^2}, \cdots \pi_i^{(0)^{e-1}} \right|^2 \qquad (i = 1, 2, \cdots e) \tag{3a}$$

dieses Fundamentalsystems genau durch

$$p^{\bar{e}-1},$$

teilbar, wenn $\bar{e}$ die Verzweigungsordnung von $\mathfrak{p}$, d. h. $\bar{e} - 1$ die Ordnungszahl von $\psi'(\pi, \eta)$ in bezug auf $\mathfrak{p}$ ist. Auch hier ist dann $\bar{e} - 1$ einfach die Ordnungszahl des Elementes $p\,i\,c_i^{(0)} \pi^{i-1}$ niedrigster Ordnung von $\psi'(\pi, \eta)$. Ist allgemeiner:

$$\psi(x, \eta^{p^k}) = x^e + p\,c_{e-1}^{(k)} x^{e-1} + \cdots + p\,c_0^{(k)} = (x - \pi_1^{(k)}) \cdots (x - \pi_e^{(k)}) = 0$$

die zu (3) konjugierte Gleichung, der die e konjugierten Primzahlen des k^{ten} Unterzyklus genügen, und

$$D(\pi^{(k)}) = \left| 1, \pi_i^{(k)}, \pi_i^{(k)^2}, \cdots \pi_i^{(k)^{e-1}} \right|^2 \tag{3b}$$

ihre Diskriminante, so ist auch sie genau durch $p^{\bar{e}-1}$ teilbar, da ja auch das zu $p\,i\,c_i^{(0)} \pi^{(0)^{i-1}}$ konjugierte Glied $p\,i\,c_i^{(k)} \pi^{(k)^{i-1}}$ die niedrigste Ordnungszahl unter den e Summanden von $\psi'(\pi^{(k)}, \eta^{p^k})$ besitzt, und da seine Ordnungszahl ebenfalls gleich $\bar{e} - 1$ ist.

Aus dem Fundamentalsystem $(1, \pi, \cdots \pi^{e-1})$ für den Koeffizientenkörper $K(\eta)$ findet man nun leicht ein Fundamentalsystem für den Bereich der rationalen p-adischen Zahlen, wenn man beachtet, daß jeder der ganzen algebraischen Koeffizienten U_i in (2c) eindeutig in der Form

$$U = u_0 + u_1 \eta + \cdots + u_{f-1} \eta^{f-1}$$

mit ganzen rationalen p-adischen Koeffizienten u_k darstellbar ist, wenn η eine primitive $(p^f - 1)^{\text{te}}$ Einheitswurzel bedeutet. Stellt man also in (2c) alle e Koeffizienten U_i in dieser Form dar, so folgt sofort, daß alle ganzen algebraischen Zahlen und nur sie eindeutig als homogene lineare Funktionen der $ef = \lambda$ Zahlen

$$(4)\quad 1, \eta, \cdots \eta^{f-1};\ \pi, \pi\eta, \cdots \pi\eta^{f-1};\ \cdots \pi^{e-1}, \pi^{e-1}\eta, \cdots \pi^{e-1}\eta^{f-1}$$

mit ganzen rationalen p-adischen Koeffizienten darstellbar sind. Diese Zahlen bilden also ein Fundamentalsystem modulo $\mathfrak{p}$ für den Körper $K(\alpha)$.

Es ist nun leicht, auch in diesem allgemeinen Falle die Potenz von $\mathfrak{p}$ zu ermitteln, welche in der Körperdiskriminante enthalten ist. Zu diesem Zwecke bilde ich die Determinante aus den λ^2 zu den Elementen (4) konjugierten algebraischen Zahlen, deren Quadrat ja die Körperdiskriminante in bezug auf $\mathfrak{p}$ ist. Sind allgemein $(\pi_1^{(i)}, \pi_2^{(i)}, \cdots \pi_e^{(i)})$ für $(i = 0, 1, \cdots f - 1)$ die zu π konjugierten Zahlen und bezeichnet man zur Abkürzung die konjugierten Zahlen $\left(\eta, \eta^p, \cdots \eta^{p^{f-1}}\right)$ durch $(\eta^{(0)}, \eta^{(1)}, \ldots \eta^{(f-1)})$, so erhält man die folgende Determinante:

$$(4\text{a})\quad \Delta(\eta,\pi) = \left|\left(\eta^{(i)^l}\cdot \pi_k^{(i)^m}\right)\right| = \left|\begin{array}{l} \left.\begin{array}{c} \ldots\ \eta^{(0)^l}\,\pi_1^{(0)^m}\ \ldots\ldots \\ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot \\ \ldots\ \eta^{(0)^l}\,\pi_e^{(0)^m}\ \ldots\ldots \end{array}\right\}\ e \text{ Zeilen} \\ \left.\begin{array}{c} \ldots\ \eta^{(1)^l}\,\pi_1^{(1)^m}\ \ldots\ldots \\ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot \\ \ldots\ \eta^{(1)^l}\,\pi_e^{(1)^m}\ \ldots\ldots \end{array}\right\}\ e \text{ Zeilen} \\ \quad\cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot \\ \quad\cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot \\ \left.\begin{array}{c} \ldots\ \eta^{(f-1)^l}\,\pi_1^{(f-1)^m}\ \ldots \\ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot\ \ \cdot \\ \ldots\ \eta^{(f-1)^l}\,\pi_e^{(f-1)^m}\ \ldots \end{array}\right\}\ e \text{ Zeilen} \end{array}\right| \qquad \begin{pmatrix} i, l = 0, 1, \cdots f-1 \\ m = 0, 1, \cdots e-1 \\ k = 1, 2, \cdots\ e \end{pmatrix}$$

Diese Determinante zerfällt in f Partialsysteme von je e Horizontalreihen. Betrachtet man irgend eins von diesen Systemen, etwa das erste, so erkennt man ohne weiteres, daß zwei seiner Horizontalreihen, etwa die i^{te} und die k^{te} einander gleich werden, sobald man das zugehörige $\pi_i^{(0)} = \pi_k^{(0)}$ setzt. Hieraus folgt, daß jede aus diesem ersten Partialsystem gebildete Determinante f^{ter} Ordnung dieselbe Eigenschaft besitzt und daher durch jede der Differenzen $\pi_i^{(0)} - \pi_k^{(0)}$ und somit auch durch ihr Produkt:

$$\text{(4b)}\qquad \pm\prod_{i>k}(\pi_i^{(0)}-\pi_k^{(0)})=\begin{vmatrix}1, & \pi_1^{(0)}, & \dots & \pi_1^{(0)^{e-1}}\\ 1, & \pi_2^{(0)}, & \dots & \pi_2^{(0)^{e-1}}\\ . & . & . & .\\ 1, & \pi_e^{(0)}, & \dots & \pi_e^{(0)^{e-1}}\end{vmatrix}=\left|\pi_k^{(0)^m}\right|$$

teilbar ist.

Da nun nach dem Laplaceschen Determinantensatze $\Delta(\eta, \pi)$ als homogene lineare Funktion aller Determinanten e^{ter} Ordnung dargestellt werden kann, welche aus jenem ersten Partialsysteme gebildet werden können, so ist auch $\Delta(\eta, \pi)$ selbst durch jenes Differenzenprodukt teilbar.

Die gleiche Überlegung, auf das zweite Partialsystem von $\Delta(\eta, \pi)$ angewendet, zeigt, daß die Körperdiskriminante auch durch die Determinante

$$\text{(4c)}\qquad \left|\pi_k^{(1)^m}\right|$$

teilbar ist, und durch analoges Weiterschließen ergibt sich die folgende Determinantenidentität:

$$\text{(5)}\qquad \left|\eta^{(i)^l}\cdot\pi_k^{(i)^m}\right| = G(\eta^{(i)})\cdot\left|\pi_k^{(0)^m}\right|\cdot\left|\pi_k^{(1)^m}\right|\cdots\left|\pi_k^{(f-1)^m}\right|,$$

wo $G(\eta^{(i)})$ eine ganze ganzzahlige Funktion der $\eta^{(i)}$ allein sein muß, wie die Vergleichung des Grades in bezug auf irgend ein Element $\pi_k^{(i)}$ lehrt; denn die links stehende Determinante enthält jedes Element $\pi_k^{(i)}$ offenbar höchstens im $(e-1)^{\text{ten}}$ Grade, und in den Determinanten $\left|\pi_k^{(i)^m}\right|$ tritt ja jedes ihrer Elemente genau in der $(e-1)^{\text{ten}}$ Potenz auf.

Um nun noch den Faktor $G(\eta^{(0)}, \eta^{(1)}, \cdots \eta^{(f-1)})$ in (5) zu bestimmen, welcher von den Elementen $\pi_k^{(i)}$ ganz unabhängig ist, kann ich diesen letzteren Elementen ganz beliebige spezielle Werte geben, nur müssen diese so gewählt werden, daß die rechts stehenden Determinanten $\left|\pi_k^{(i)^m}\right|$ nicht Null werden. Dieser Bedingung wird genügt, wenn ich die f Zyklen

$$(\pi_1^{(0)}, \dots \pi_e^{(0)}),\quad (\pi_1^{(1)}, \dots \pi_e^{(1)}), \dots (\pi_1^{(f-1)}, \dots \pi_e^{(f-1)})$$

als gleich annehme, so daß nur ein einziger Zyklus

$$(\pi_1, \pi_2, \dots \pi_e)$$

von e verschiedenen Elementen f Male auftritt.

Ich setze nun in der Determinante (4a) allgemein: $\pi_k^{(i)} = \pi_k$ und ordne ihre Horizontalreihen so um, daß ich die π_1 enthaltenden f Zeilen zuerst schreibe, hierauf die π_2 enthaltenden Zeilen u. s. f. Dann ergibt sich für die höchstens dem Vorzeichen nach veränderte Determinante eine neue Darstellung:

$$(6)\quad \pm\left|\eta^{(i)^l}\pi_k^{m}\right| = \left|\begin{array}{lllll} 1, & \eta^{(0)}, & \ldots\eta^{(0)^{f-1}}; & \pi_1,\ldots\pi_1\eta^{(0)^{f-1}}; & \ldots \\ 1, & \eta^{(1)}, & \ldots\eta^{(1)^{f-1}}; & \pi_1,\ldots\pi_1\eta^{(1)^{f-1}}; & \ldots \\ \vdots & & & & \\ 1, & \eta^{(f-1)}, & \ldots\eta^{(f-1)^{f-1}}; & \pi_1,\ldots\pi_1\eta^{(f-1)^{f-1}}; & \ldots \\ 1, & \eta^{(0)}, & \ldots\eta^{(0)^{f-1}}; & \pi_2,\ldots\pi_2\eta^{(0)^{f-1}}; & \ldots \\ \vdots & & & & \\ 1, & \eta^{(f-1)}, & \ldots\eta^{(f-1)^{f-1}}; & \pi_2,\ldots\pi_2\eta^{(f-1)^{f-1}}; & \ldots \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{array}\right| \begin{array}{l} \left.\right\} f \text{ Zeilen.} \\ \\ \left.\right\} f \text{ Zeilen.} \end{array}$$

Betrachtet man nun wieder eins unter diesen neuen Partialsystemen von je f Zeilen, etwa das erste, und beachtet, daß jetzt in diesem die i^{te} Zeile gleich der k^{ten} wird, wenn man die bezüglichen Elemente $\eta^{(i)}$ und $\eta^{(k)}$ einander gleichsetzt, und daß dasselbe also für jede Determinante f^{ter} Ordnung der Fall ist, welche man aus diesem ersten Partialsystem bilden kann, so findet man wieder, daß jede dieser Determinanten durch die Diskriminante:

$$(6\text{a})\qquad \pm\prod_{i>k}(\eta^{(i)}-\eta^{(k)}) = \left|\begin{array}{lll} 1, & \eta^{(0)}, & \ldots\eta^{(0)^{f-1}} \\ 1, & \eta^{(1)}, & \ldots\eta^{(1)^{f-1}} \\ \vdots & & \\ 1, & \eta^{(f-1)}, & \ldots\eta^{(f-1)^{f-1}} \end{array}\right| = \left|\eta^{(i)^l}\right|$$

der f Elemente $(\eta^{(0)},\ldots\eta^{(f-1)})$ teilbar ist. Das gleiche gilt aber auch für jede Determinante f^{ter} Ordnung des zweiten, dritten, ... e^{ten} Partialsystemes. Entwickelt man nun die Determinante (6), dem Laplaceschen Satze gemäß zuerst nach den Determinanten des ersten Partialsystems, so stellt sie sich als eine Summe dar:

$$\left|\eta^{(i)^l}\pi_k^{m}\right| = \sum \varDelta_1\overline{\varDelta_1},$$

deren Elemente $\varDelta_1$ alle jene Determinanten f^{ten} Grades des ersten Systemes bedeuten, und wo $\overline{\varDelta_1}$ jedesmal die zugehörige komplementäre Determinante $(\lambda-f)^{\text{ten}}$ Grades ist, welche aus den $\lambda-f$ letzten Horizontalreihen gebildet wird. Entwickelt man nun jede dieser komplementären Determinanten $\overline{\varDelta_1}$ in gleicher Weise nach den Determinanten des zweiten Partialsystems und fährt so fort, so ergibt sich schließlich für unsere Determinante die folgende Darstellung:

$$\left|\eta^{(i)^l}\pi_k^{m}\right| = \sum \varepsilon\varDelta_1\,\varDelta_2\ldots\varDelta_e,$$

wo $\varDelta_1$ alle Determinanten f^{ter} Ordnung des ersten Partialsystemes, $\varDelta_2$ alle Determinanten des zweiten, ... $\varDelta_e$ endlich alle Determinanten des

e^{ten} Partialsystemes durchläuft, und die ε gewisse Zahlkoeffizienten sind. Da nun, wie soeben bewiesen wurde, jede dieser Determinanten Δ_i durch die Determinante $|\eta^{(i)^l}|$ teilbar ist, so folgt, daß die zu untersuchende Determinante durch $|\eta^{(i)^l}|^e$ teilbar ist, daß also eine Gleichung besteht:

$$(7) \qquad |\eta^{(i)^l}\pi_k{}^m| = |\eta^{(i)^l}|^e \cdot H(\pi_k),$$

und eine Vergleichung der Grade beider Seiten in bezug auf die $\eta^{(i)}$ lehrt wieder, daß der zweite Koeffizient $H(\pi^{(k)})$ kein $\eta^{(i)}$ mehr enthalten kann, da nur dann beide Seiten in bezug auf jedes $\eta^{(i)}$ vom $e(f-1)^{\text{ten}}$ Grade sind. Also ergibt sich für die noch zu bestimmende ganze Funktion $G(\eta^{(i)})$ in (5) der Wert $\varepsilon \cdot |\eta^{(i)^l}|^e$, wo ε eine noch unbekannte ganze Zahl bedeutet; so erhält man die folgende interessante Determinantenidentität:

$$(8) \qquad \sqrt{D} = |\eta^{(i)^l}\pi_k^{(i)^m}| = \varepsilon\, |\eta^{(i)^l}|^e \cdot \prod_{i=0}^{f-1} |\pi_k^{(i)^m}|,$$

und die Vergleichung z. B. der Diagonalglieder auf beiden Seiten lehrt endlich, daß $\varepsilon = \pm 1$ sein muß.

Diese wichtige Identität ergibt nun sofort die in der Körperdiskriminante D enthaltene Potenz von $\mathfrak{p}$: Zunächst enthält weder ε noch die Determinante:

$$|\eta^{(i)^l}| = \pm \prod_{i>k} (\eta^{p^i} - \eta^{p^k})$$

den Divisor $\mathfrak{p}$, weil ja die f konjugierten Einheitswurzeln

$$(\eta, \eta^p, \ldots \eta^{p^{f-1}})$$

modulo $\mathfrak{p}$ inkongruent sind. Ferner ist jedes der f Determinantenquadrate

$$|\pi_k^{(i)^m}|^2 = \pm \prod (\pi_g^{(i)} - \pi_k^{(i)}) = \pm\, n(\psi'(\pi^{(i)}, \eta^{(i)}))$$

nach dem a. S. 221 bewiesenen Satze durch dieselbe Potenz von $\mathfrak{p}$, nämlich durch

$$\mathfrak{p}^{e\cdot(\bar{e}-1)} \sim p^{\bar{e}-1}$$

teilbar, wenn wieder $\bar{e}$ die Verzweigungsordnung von $\mathfrak{p}$ bedeutet. Also ist die in D enthaltene Potenz von p d. h. der zu $\mathfrak{p}$ gehörige Diskriminantenteiler:

$$(9) \qquad D(\mathfrak{p}) = p^{f(\bar{e}-1)} = n(\mathfrak{p}^{\bar{e}-1}).$$

Im allgemeinen ist die Verzweigungsordnung $\bar{e}$ gleich der Ordnung e des Primteilers $\mathfrak{p}$; sie ist dann und nur dann größer als e, wenn

$$e = p^s e_0$$

durch p teilbar ist; und zwar liegt sie dann zwischen $e + 1$ und $(s + 1)e$. Da also stets $\bar{e} \geqq e$ ist, so ist die Körperdiskriminante modulo $\mathfrak{p}$ dann und nur dann durch $\mathfrak{p}$ garnicht teilbar, wenn $\bar{e}$, also auch die Ordnung e gleich Eins, d. h. wenn $\mathfrak{p}$ kein Verzweigungsteiler von $K(\alpha)$ ist. Hierdurch wird der a. S. 216 ausgesprochene Satz neu bewiesen.

Ich spreche die wichtigen Ergebnisse dieser letzten Betrachtung in dem folgenden Satze aus:

> Ist $\mathfrak{p}$ ein beliebiger Primteiler der reellen Primzahl p für den Körper $K(\alpha)$, und sind f, e und $\bar{e}$ der Grad, die Ordnung und die Verzweigungsordnung von $\mathfrak{p}$, so kann man stets ein Fundamentalsystem modulo $\mathfrak{p}$ von $\lambda = ef$ modulo $\mathfrak{p}$ ganzen algebraischen Zahlen:
>
> (10) $$\gamma^{(1)}, \gamma^{(2)}, \ldots \gamma^{(\lambda)}$$
>
> finden, und seine Diskriminante:
>
> $$D = |\gamma_k^{(i)}|^2$$
>
> ist genau durch $D(\mathfrak{p}) = n(\mathfrak{p}^{\bar{e}-1})$ teilbar.

Ich benutze dieses Resultat, um eine sehr viel allgemeinere Folgerung herzuleiten. Ich betrachte den Bereich aller algebraischen Zahlen von $K(\alpha)$, welche durch $\mathfrak{p}^r$ teilbar sind, wo r eine beliebige ganze Zahl bedeutet. Ist $r = 0$, so ist das in (10) gefundene Fundamentalsystem:

$$\gamma^{(1)}, \gamma^{(2)}, \ldots \gamma^{(\lambda)}$$

ein Fundamentalsystem für alle durch $\mathfrak{p}^0$ teilbaren Zahlen. Ist dagegen $r \gtrless 0$, so bildet offenbar dasjenige System

(11) $$\bar{\gamma}^{(1)}, \bar{\gamma}^{(2)}, \ldots \bar{\gamma}^{(\lambda)}$$

in gleichem Sinne ein Fundamentalsystem für alle Multipla von $\mathfrak{p}^r$, dessen Elemente

(11a) $$\bar{\gamma}^{(i)} = \pi^r \gamma^{(i)}$$

sind. In der Tat ist ja jede durch $\mathfrak{p}^r$ teilbare Zahl $\bar{\gamma}$ auf eine einzige Weise in der Form $\pi^r \gamma$ darstellbar, wo γ algebraisch ganz ist, d. h. es ist:

$$\bar{\gamma} = \pi^r \gamma = \pi^r(u_1 \gamma^{(1)} + \cdots + u_\lambda \gamma^{(\lambda)}) = u_1 \bar{\gamma}^{(1)} + \cdots + u_\lambda \bar{\gamma}^{(\lambda)},$$

wo die u_i ganze rationale p-adische Zahlen sind; unsere Behauptung ist also vollständig bewiesen.

In jedem Körper $K(\alpha)$ kann man also stets ein Fundamentalsystem für die Vielfachen von $\mathfrak{p}^r$ finden, wenn $\mathfrak{p}$ irgend einen Prim-

teiler, und r einen beliebigen positiven, negativen oder verschwindenden Exponenten bedeutet. Ist $(\bar{\delta}^{(1)}, \bar{\delta}^{(2)}, \ldots \bar{\delta}^{(\lambda)})$ irgend ein anderes System von Vielfachen von $\mathfrak{p}^r$, so sind seine Elemente $\bar{\delta}^{(i)}$ durch das Fundamentalsystem $(\bar{\gamma}^{(1)}, \ldots \bar{\gamma}^{(\lambda)})$ in der Form:

(12) $$\bar{\delta}^{(i)} = \sum c_{ik} \bar{\gamma}^{(k)}$$

mit ganzzahligen p-adischen Koeffizienten darstellbar; und hieraus folgt genau ebenso, wie a. S. 116, daß das System $(\bar{\delta}^{(1)}, \ldots \bar{\delta}^{(\lambda)})$ dann und nur dann ebenfalls ein Fundamentalsystem für die Multipla von $\mathfrak{p}^r$ ist, wenn die Substitutionsdeterminante $|c_{ik}|$ durch p nicht teilbar ist. Beachtet man ferner, daß die Gleichungen (12) richtig bleiben, wenn man zu den λ konjugierten Zahlen übergeht; so ergeben sich die λ^2 Gleichungen

$$\bar{\delta}_l^{(i)} = \sum_k c_{ik} \bar{\gamma}_l^{(k)},$$

und durch Übergang zu den Determinanten erhält man genau wie a. S. 117 (6) die Relation:

(11a) $$|\bar{\delta}_l^{(i)}|^2 = |c_{ik}|^2 \, |\bar{\gamma}_l^{(k)}|^2.$$

Ist also $(\bar{\gamma}^{(1)}, \ldots \bar{\gamma}^{(\lambda)})$ irgend ein Fundamentalsystem für die Multipla von $\mathfrak{p}^r$ und $(\bar{\delta}^{(1)}, \ldots \bar{\delta}^{(\lambda)})$ irgend ein anderes System von Vielfachen von $\mathfrak{p}^r$, so ist dasselbe dann und nur dann ebenfalls ein Fundamentalsystem für die Multipla von $\mathfrak{p}^r$, wenn seine Diskriminante keine höhere Potenz von $\mathfrak{p}$ enthält als die Diskriminante des ersten Systemes. Ein System von λ Vielfachen von $\mathfrak{p}^r$ ist also dann und nur dann ein Fundamentalsystem für diese Multipla, wenn seine Diskriminante eine möglichst niedrige Potenz von $\mathfrak{p}$ enthält.

Ich nenne die in dieser Diskriminante enthaltene Potenz von p den zu $\mathfrak{p}^r$ gehörigen Diskriminantenteiler und bezeichne ihn durch $D(\mathfrak{p}^r)$. Hiernach ist der a. S. 215 eingeführte Diskriminantenteiler $D(\mathfrak{p}) = p^{f(e-1)}$ in Zukunft durch $D(\mathfrak{p}^0)$ zu bezeichnen, weil er ja dem Exponenten $r = 0$ entspricht.

Es ist jetzt sehr leicht, die in der Diskriminante:

$$\begin{vmatrix} \bar{\gamma}_1^{(1)}, & \bar{\gamma}_1^{(2)}, & \ldots \bar{\gamma}_1^{(\lambda)}, \\ \bar{\gamma}_2^{(1)}, & \bar{\gamma}_2^{(2)}, & \ldots \bar{\gamma}_2^{(\lambda)}, \\ \vdots & & \\ \bar{\gamma}_\lambda^{(1)}, & \bar{\gamma}_\lambda^{(2)}, & \ldots \bar{\gamma}_\lambda^{(\lambda)}, \end{vmatrix}^2 = \begin{vmatrix} \gamma_1^{(1)} \pi_1^r, & \gamma_1^{(2)} \pi_1^r, & \ldots \gamma_1^{(\lambda)} \pi_1^r, \\ \gamma_2^{(1)} \pi_2^r, & \gamma_2^{(2)} \pi_2^r, & \ldots \gamma_2^{(\lambda)} \pi_2^r, \\ \vdots & & \\ \gamma_\lambda^{(1)} \pi_\lambda^r, & \gamma_\lambda^{(2)} \pi_\lambda^r, & \ldots \gamma_\lambda^{(\lambda)} \pi_\lambda^r \end{vmatrix}^2$$

enthaltene Potenz $D(\mathfrak{p}^r)$ von p zu bestimmen. Zieht man nämlich aus der ersten, zweiten, … λ^{ten} Zeile der zweiten Determinante der Reihe nach $\pi_1^r, \pi_2^r, \ldots \pi_\lambda^r$ heraus, so geht sie in die Determinante des Fundamental-

systemes $(\gamma^{(1)}, \gamma^{(2)}, \ldots \gamma^{(\lambda)})$ für die modulo $\mathfrak{p}$ ganzen Zahlen über, dessen Diskriminante soeben bestimmt und äquivalent $n(\mathfrak{p}^{\bar{e}-1})$ gefunden wurde. Beachtet man ferner, daß das herausgezogene Produkt

$$((\pi_1 \pi_2 \ldots \pi_\lambda)^r)^2 \sim n(\mathfrak{p}^r)^2 \sim n(\mathfrak{p}^{2r})$$

ist, so ergibt sich der wichtige Satz:

Für den zu einer beliebigen Divisorenpotenz $\mathfrak{p}^r$ gehörenden Diskriminantenteiler $D(\mathfrak{p}^r)$ besteht die Gleichung:

(13) $$D(\mathfrak{p}^r) = n(\mathfrak{p}^{2r+\bar{e}-1}) = p^{f(2r+\bar{e}-1)};$$

oder da für $r=0$, d. h. für den Diskriminantenteiler $D(\mathfrak{p}^0)$ eines Fundamentalsystemes für die modulo $\mathfrak{p}$ ganzen algebraischen Zahlen:

(13a) $$D(\mathfrak{p}^0) = n(\mathfrak{p}^{\bar{e}-1})$$

ist, so kann die obige Gleichung auch in der Form:

(13b) $$D(\mathfrak{p}^r) = (n(\mathfrak{p}^r))^2 \cdot D(\mathfrak{p}^0)$$

geschrieben werden.

§ 4. Bestimmung derjenigen Potenz einer beliebigen Primzahl p, welche in der Körperdiskriminante enthalten ist.

Die im vorigen Abschnitte gefundenen Ergebnisse können nun benutzt werden, um aus den Fundamentalsystemen für die einzelnen Primteiler einer reellen Primzahl p ein Fundamentalsystem für diese Primzahl p selbst zusammenzusetzen.

Ich nehme der Einfachheit wegen wieder, wie a. S. 160, an, p besitze nur drei voneinander verschiedene Primteiler $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$, so daß die linke Seite der Grundgleichung n^{ten} Grades für den Bereich der rationalen p-adischen Zahlen in drei irreduktible Faktoren zerfällt. Es sei:

(1) $$F(x) = f(x) \cdot g(x) \cdot h(x) \quad (p)$$

diese Zerlegung, und λ, μ und ν seien wieder die Grade jener Faktoren, so daß $\lambda + \mu + \nu = n$ ist. Die n Wurzeln dieser Gleichung für den Bereich von p zerfallen dann in die drei Zyklen von konjugierten p-adischen Zahlen

(1a) $$\alpha_1, \ldots \alpha_\lambda; \quad \alpha_{\lambda+1}, \ldots \alpha_{\lambda+\mu}; \quad \alpha_{\lambda+\mu+1}, \ldots \alpha_n,$$

welche bzw. den Primteilern $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ entsprechen. Dann besteht der folgende wichtige Satz:

Es seien

$$\gamma_1, \gamma_2, \ldots \gamma_\lambda; \quad \delta_1, \delta_2, \ldots \delta_\mu; \quad \varepsilon_1, \varepsilon_2, \ldots \varepsilon_\nu$$

drei beliebige Zyklen von je λ, μ und ν konjugierten algebraischen p-adischen Zahlen für den Bereich von $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$.

Dann kann man stets eine p-adische Zahl β innerhalb $K(\alpha)$ so bestimmen, daß ihre n Konjugierten

$$\beta_1, \beta_2, \dots \beta_\lambda; \quad \beta_{\lambda+1} \dots \beta_{\lambda+\mu}; \quad \beta_{\lambda+\mu+1} \dots \beta_n$$

für den Bereich von $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ bzw. gleich

$$\gamma_1, \gamma_2, \dots \gamma_\lambda; \qquad \delta_1, \dots \delta_\mu; \qquad \varepsilon_1, \dots \varepsilon_\nu$$

werden, d. h. daß ihre drei Wurzelzyklen beliebig vorgegebene konjugierte Entwicklungen haben.

Zum Beweise genügt es, wie gleich gezeigt werden wird, $\gamma = 1$, $\delta = \varepsilon = 0$ anzunehmen. Bezeichnen wir nun das Produkt $g(x)\,h(x)$ in (1) durch $f_1(x)$, so sind die beiden Funktionen $f(x)$ und $f_1(x)$ teilerfremd; man kann also durch das Euklidische Verfahren zwei komplementäre Faktoren $\bar{f}(x)$ und $\bar{f}_1(x)$ so bestimmen, daß:

$$f(x)\,\bar{f}(x) + f_1(x)\,\bar{f}_1(x) = 1 \quad (p)$$

ist. Setzt man dann:

$$G(x) = f_1(x)\,\bar{f}_1(x) = 1 - f(x)\,\bar{f}(x), \tag{2}$$

so ist $G(x)$ eine ganze Funktion von x mit rationalen p-adischen Koeffizienten, welche die gesuchte Eigenschaft besitzt. Ersetzt man nämlich x durch eine der Zahlen $\alpha_1, \dots \alpha_\lambda$, so folgt aus der zweiten Darstellung von $G(x)$ in (2), daß:

$$G(\alpha_1) = G(\alpha_2) = \cdots = G(\alpha_\lambda) = 1 \tag{3}$$

ist. Setzt man dagegen x gleich einer der Wurzeln $\alpha_{\lambda+r}$ von:

$$f_1(x) = g(x)\,h(x) = 0,$$

so folgt aus der ersten Darstellung von $G(x)$ in (2), daß:

$$G(\alpha_{\lambda+1}) = \cdots = G(\alpha_n) = 0 \tag{3a}$$

ist; unsere Behauptung ist also bewiesen.

In derselben Weise denke ich mir nun drei p-adische algebraische Zahlen $d_{100}, d_{010}, d_{001}$ von $K(\alpha)$ so bestimmt, daß für d_{100} der zu $\mathfrak{p}_1$ gehörige Wurzelzyklus gleich Eins ist, und ebenso für d_{010} der zu $\mathfrak{p}_2$, für d_{001} der zu $\mathfrak{p}_3$ gehörige Zyklus gleich Eins wird, während jedesmal die beiden übrigen Zyklen gleich Null sind. Sind dann γ, δ und ε drei ganz beliebige Zahlen von $K(\alpha)$, so ist die Zahl:

$$\beta = \gamma d_{100} + \delta d_{010} + \varepsilon d_{001} \tag{4}$$

so beschaffen, daß ihr zu $\mathfrak{p}_1$ gehöriger Wurzelzyklus mit dem entsprechenden von γ, der zu $\mathfrak{p}_2$ bzw. $\mathfrak{p}_3$ gehörige Zyklus mit dem ent-

sprechenden von δ bzw. ε übereinstimmt. Damit ist also unser Fundamentalsatz in seiner allgemeinsten Form bewiesen.

Es sei nun

$$(5)\qquad \gamma^{(1)}, \gamma^{(2)}, \ldots \gamma^{(\lambda)};\quad \delta^{(1)}, \delta^{(2)}, \ldots \delta^{(\mu)};\quad \varepsilon^{(1)}, \varepsilon^{(2)}, \ldots \varepsilon^{(\nu)}$$

je ein Fundamentalsystem für die ganzen algebraischen Zahlen von $K(\alpha)$ in bezug auf die drei Primteiler $\mathfrak{p}_1$, $\mathfrak{p}_2$ und $\mathfrak{p}_3$. Dann bleiben diese drei Systeme Fundamentalsysteme, wenn ich die Elemente $\gamma^{(i)}$ des ersten mit d_{100}, die Elemente $\delta^{(i)}$ und $\varepsilon^{(i)}$ bzw. mit d_{010} und d_{001} multipliziere, denn jene drei Multiplikatoren $d_{100}, d_{010}, d_{001}$ sind ja für den Bereich von $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ bzw. gleich Eins, für die beiden anderen Divisoren aber immer gleich Null. Nach erfolgter Multiplikation mit jenen drei Zahlen will ich dieselben wieder durch die gleichen Buchstaben bezeichnen. Dann behaupte ich, daß die so gewonnenen Zahlen (5) zusammengenommen ein Fundamentalsystem modulo p bilden, d. h. daß eine Summe mit rationalen p-adischen Koeffizienten:

$$(6)\qquad \beta = u_1\gamma^{(1)} + \cdots + u_\lambda\gamma^{(\lambda)} + v_1\delta^{(1)} + \cdots + v_\mu\delta^{(\mu)} + w_1\varepsilon^{(1)} + \cdots + w_\nu\varepsilon^{(\nu)}$$

dann und nur dann algebraisch ganz ist, wenn die n Koeffizienten u_i, v_k, w_l sämtlich **ganze** rationale p-adische Zahlen sind. Man erkennt zunächst, daß die Determinante dieses Systemes von Null verschieden, daß also jenes System eine Basis modulo p für den Körper $K(\alpha)$ ist. Diese Determinante ist nämlich gleich:

$$(7)\qquad \begin{vmatrix} \gamma_1^{(1)} & \ldots & \gamma_1^{(\lambda)} & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & & & & & & & & \\ \gamma_\lambda^{(1)} & \ldots & \gamma_\lambda^{(\lambda)} & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & \ldots & 0 & \delta_1^{(1)} & \ldots & \delta_1^{(\mu)} & 0 & \ldots & 0 \\ \vdots & & & \vdots & & & & & \\ 0 & \ldots & 0 & \delta_\mu^{(1)} & \ldots & \delta_\mu^{(\mu)} & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & \ldots & 0 & \varepsilon_1^{(1)} & \ldots & \varepsilon_1^{(\nu)} \\ \vdots & & \vdots & \vdots & & & \vdots & & \\ 0 & \ldots & 0 & 0 & \ldots & 0 & \varepsilon_\nu^{(1)} & \ldots & \varepsilon_\nu^{(\nu)} \end{vmatrix} = \left|\gamma_{k_1}^{(i_1)}\right| \left|\delta_{k_2}^{(i_2)}\right| \left|\varepsilon_{k_3}^{(i_3)}\right|,$$

weil die zu $\mathfrak{p}_2$ bzw. $\mathfrak{p}_3$ gehörigen Entwicklungen für $(\gamma^{(1)}, \ldots \gamma^{(\lambda)})$ gleich Null sind usw.

Also ist jede Zahl β von $K(\alpha)$ für den Bereich von p auf eine einzige Weise in der Form (6) mit rationalen p-adischen Koeffizienten darstellbar, und diese Zahl ist dann und nur dann modulo p algebraisch ganz, wenn sie für den Bereich von $\mathfrak{p}_1$, $\mathfrak{p}_2$ und $\mathfrak{p}_3$ ganz ist. Da nun

z. B. für den Bereich von $\mathfrak{p}_1$ die Zahlen $\delta^{(i)}$ und $\varepsilon^{(k)}$ gleich Null sind, so besteht für die λ zu $\mathfrak{p}_1$ gehörigen konjugierten Zahlen $\beta_1, \ldots \beta_\lambda$ für diesen Bereich die Darstellung:

$$\beta_i = u_1 \gamma_i^{(1)} + \cdots + u_\lambda \gamma_i^{(\lambda)} \quad (\mathfrak{p}_1) \qquad (i = 1, 2, \cdots \lambda),$$

und da $(\gamma^{(1)}, \ldots \gamma^{(\lambda)})$ n. d. V. ein Fundamentalsystem ist, so ist β dann und nur dann modulo $\mathfrak{p}_1$ ganz, wenn $u_1, \ldots u_\lambda$ ganze p-adische Zahlen sind. Genau ebenso zeigt man, daß β nur dann modulo $\mathfrak{p}_2$ bzw. $\mathfrak{p}_3$ algebraisch ganz ist, wenn alle Koeffizienten $v_1, \ldots v_\mu$ bzw. $w_1, \ldots w_\nu$ ganze p-adische Zahlen sind; damit ist also unsere Behauptung vollständig bewiesen.

Nun kann man leicht die in der Körperdiskriminante von $K(\alpha)$ enthaltene Potenz $D(p)$ der Primzahl p bestimmen: Erhebt man nämlich die Determinantenrelation (7) zum Quadrate, so ergibt sich links die Diskriminante des Fundamentalsystemes (5) modulo p, rechts das Produkt der Körperdiskriminanten modulo $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$. Man erhält also den Satz, welchen ich gleich für den Fall ausspreche, daß p h verschiedene Primteiler innerhalb $K(\alpha)$ besitzt:

Die in der Körperdiskriminante von $K(\alpha)$ enthaltene Potenz einer beliebigen Primzahl p ist stets gleich dem Produkte aller zu den verschiedenen Primfaktoren von p gehörigen Diskriminantenteilern, d. h. es ist:

$$(8) \qquad D(p) = \prod_{\mathfrak{p}_i | p} D(\mathfrak{p}_i^0) = \prod p^{f_i(\bar{e}_i - 1)} = n\,(\Pi \mathfrak{p}_i^{\bar{e}_i - 1}),$$

wenn:

$$(8\text{a}) \qquad p = \prod_{i=1}^{h} \mathfrak{p}_i^{e_i}$$

ist, und allgemein f_i den Grad, $\bar{e}_i$ die Verzweigungsordnung des Primteilers $\mathfrak{p}_i$ bedeutet.

Umgekehrt ist ein System von modulo p ganzen algebraischen Zahlen, dessen Diskriminante genau durch $p^{\Sigma f_i(\bar{e}_i - 1)}$ teilbar ist, stets ein Fundamentalsystem modulo p.

Ist speziell die Primzahl p in keiner der Ordnungszahlen e_i ihrer Primteiler $\mathfrak{p}_i$ als Divisor enthalten, so ist allgemein:

$$\bar{e}_i = e_i,$$

und da $e_1 f_1 + \cdots + e_h f_h = n$ ist, so folgt daß in diesem Falle $D(p)$ genau gleich:

$$p^{n-f}$$

ist, wo:

$$(8\text{b}) \qquad f = f_1 + f_2 + \cdots + f_h$$

die Summe der Grade aller verschiedenen Primteiler von p bedeutet. Ist dagegen auch nur eine der Ordnungszahlen e_i durch p teilbar, so ist $D(p)$ sicher größer als p^{n-f}.

Endlich enthält die Körperdiskriminante die Primzahl p dann und nur dann garnicht, wenn jeder der h Primteiler $\mathfrak{p}_i$ von der Ordnung $e_i = 1$, wenn also kein einziger unter ihnen ein Verzweigungsteiler ist.

> Dann und nur dann ist also p kein Teiler der Körperdiskriminante von $K(\alpha)$, wenn alle für den Bereich von p konjugierten p-adischen Zahlen dieses Körpers nach ganzen Potenzen von p fortschreiten.

Es seien nun wieder $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ die in der Primzahl p enthaltenen von einander verschiedenen Primteiler, dann will ich jetzt allgemeiner alle diejenigen Zahlen von $K(\alpha)$ betrachten, welche durch ein beliebiges Produkt

$$\mathfrak{d} = \mathfrak{p}_1^{r_1}\,\mathfrak{p}_2^{r_2}\,\mathfrak{p}_3^{r_3} \tag{9}$$

von Potenzen dieser Divisoren teilbar sind, welche also in bezug auf $\mathfrak{p}_1$ bzw. $\mathfrak{p}_2$ und $\mathfrak{p}_3$ mindestens die Ordnungszahlen r_1 bzw. r_2 und r_3 besitzen. Auch für diese Zahlen können wir sehr leicht ein Fundamentalsystem aus den Fundamentalsystemen für die Divisoren $\mathfrak{p}_1^{r_1}, \mathfrak{p}_2^{r_2}, \mathfrak{p}_3^{r_3}$ zusammensetzen. In der Tat, seien die $n = \lambda + \mu + \nu$ Zahlen:

$$\bar{\gamma}^{(1)}, \ldots \bar{\gamma}^{(\lambda)};\quad \bar{\delta}^{(1)}, \ldots \bar{\delta}^{(\mu)};\quad \bar{\varepsilon}^{(1)}, \ldots \bar{\varepsilon}^{(\nu)} \tag{10}$$

wieder Fundamentalsysteme bzw. für die Multipla der drei Divisorenpotenzen

$$\mathfrak{p}_1^{r_1}, \quad \mathfrak{p}_2^{r_2}, \quad \mathfrak{p}_3^{r_3},$$

wie sie a. S. 226 flgde. bestimmt wurden, und zwar seien sie wieder wie a. S. 230 von vornherein so angenommen, daß die $\mu + \nu$ für den Bereich von $\mathfrak{p}_2$ und $\mathfrak{p}_3$ zu $\bar{\gamma}^{(1)}, \ldots \bar{\gamma}^{(\lambda)}$ konjugierten Zahlen gleich Null sind, und daß das entsprechende für die beiden anderen Partialsysteme $(\bar{\delta}^{(1)}, \ldots \bar{\delta}^{(\mu)})$ und $(\bar{\varepsilon}^{(1)}, \ldots \bar{\varepsilon}^{(\nu)})$ gilt. Dann beweist man wörtlich ebenso, wie für das System (5) a. S. 230, daß auch die n Zahlen (10) für den Divisor $\mathfrak{d}$ ein Fundamentalsystem bilden, daß nämlich eine Zahl:

$$\bar{\beta} = u_1\bar{\gamma}^{(1)} + \cdots + u_\lambda\bar{\gamma}^{(\lambda)} + v_1\bar{\delta}^{(1)} + \cdots + v_\mu\bar{\delta}^{(\mu)} + w_1\bar{\varepsilon}^{(1)} + \cdots + w_\nu\bar{\varepsilon}^{(\nu)} \tag{11}$$

dann und nur dann durch $\mathfrak{d}$ teilbar ist, wenn die n Koeffizienten u_i, v_k, w_l sämtlich ganze rationale p-adische Zahlen sind. Auch hier ist nämlich die Determinante dieses Systemes genau wie in (7) a. S. 230

$$\left|\bar{\gamma}_m^{(i)}, \quad \bar{\delta}_m^{(k)}, \quad \bar{\varepsilon}_m^{(l)}\right| = \left|\bar{\gamma}_{k_1}^{(i_1)}\right| \cdot \left|\bar{\delta}_{k_2}^{(i_2)}\right| \cdot \left|\bar{\varepsilon}_{k_3}^{(i_3)}\right|, \tag{12}$$

also von Null verschieden; daher ist jede Zahl $\bar{\beta}$ sicher in der Form (11) mit ganzen oder gebrochenen Koeffizienten u_i darstellbar. Soll aber $\bar{\beta}$ durch $\mathfrak{p}_1^{r_1}$ teilbar sein, und beachtet man, daß auch jetzt für den Bereich von $\mathfrak{p}_1$ die Zahlen $\bar{\delta}^{(i)}$ und $\bar{\varepsilon}^{(k)}$ Null sind, so folgt, daß wieder:

$$\bar{\beta} \equiv u_1 \bar{\gamma}^{(1)} + \cdots + u_\lambda \bar{\gamma}^{(\lambda)} \equiv 0 \quad \left(\operatorname{mod} \mathfrak{p}_1^{r_1}\right),$$

sein muß, was dann und nur dann möglich ist, wenn die Koeffizienten $u_1, \ldots u_\lambda$ ganze p-adische Zahlen sind; und da genau das Entsprechende für die Koeffizienten v_k und w_l gilt, so ist unsere Behauptung vollständig bewiesen.

Erhebt man die Determinantenrelation (12) zum Quadrat, so folgt genau wie in (8) die Gleichung:

$$D(\mathfrak{d}) = D\left(\mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\mathfrak{p}_3^{r_3}\right) = D\left(\mathfrak{p}_1^{r_1}\right) D\left(\mathfrak{p}_2^{r_2}\right) D\left(\mathfrak{p}_3^{r_3}\right), \tag{13}$$

wo $D(\mathfrak{d})$ wieder die in der Diskriminante (12) des Fundamentalsystemes für den Divisor $\mathfrak{d}$ enthaltene Potenz von p bedeutet; und da nach der a. S. 228 bewiesenen Gleichung (13b):

$$D\left(\mathfrak{p}_i^{r_i}\right) = n\left(\mathfrak{p}_i^{r_i}\right)^2 \cdot D\left(\mathfrak{p}_i^{0}\right) \tag{13a}$$

ist, so ergibt sich die Gleichung:

$$D(\mathfrak{d}) = n(\mathfrak{d}^2)\, D(p), \tag{13b}$$

wenn $D(p)$ wieder die Potenz von p bedeutet, welche in der Diskriminante des Fundamentalsystems für die modulo p ganzen algebraischen Zahlen enthalten ist.

Ist $(\xi^{(1)}, \ldots \xi^{(n)})$ irgend ein Fundamentalsystem für die Multipla von $\mathfrak{d}$, etwa das in (10) betrachtete $\left(\bar{\gamma}^{(i)}, \bar{\delta}^{(k)}, \bar{\varepsilon}^{(l)}\right)$, und sind $(\eta^{(1)}, \ldots \eta^{(n)})$ n andere Multipla von $\mathfrak{d}$, so sind die Elemente $\eta^{(i)}$ durch das System $(\xi^{(1)}, \ldots \xi^{(n)})$ in der Form:

$$\eta^{(i)} = \sum c_{ik}\, \xi^{(k)}$$

mit ganzzahligen p-adischen Koeffizienten darstellbar, und man zeigt genau ebenso wie a. S. 116, daß das System $(\eta^{(1)}, \ldots \eta^{(n)})$ dann und nur dann ebenfalls ein Fundamentalsystem für denselben Divisor ist, wenn die ganzzahlige Determinante $|c_{ik}|$ eine Einheit modulo p ist. Da nun die Diskriminanten jener beiden Systeme durch die Gleichung:

$$D(\eta^{(i)}) = |c_{ik}|^2 \cdot D(\xi^{(i)})$$

zusammenhängen, so folgt, daß je zwei Fundamentaldiskriminanten für denselben Divisor $\mathfrak{d}$ dieselbe Potenz $D(\mathfrak{d})$ von p enthalten. Es gilt also der Satz:

Ein System von n Vielfachen von $\mathfrak{d} = \mathfrak{p}_1^{r_1} \mathfrak{p}_2^{r_2} \mathfrak{p}_3^{r_3}$ ist dann und nur dann ein Fundamentalsystem für diesen Divisor, wenn seine Diskriminante durch die kleinstmögliche Potenz von p, nämlich genau durch

$$(13\text{b}) \qquad D(\mathfrak{d}) = n(\mathfrak{d}^2)\, D(p) = n(\mathfrak{d}^2)\, n(\Pi(\mathfrak{p}_i^{\bar{e}_i - 1}))$$

teilbar ist.

§ 5. Die vollständige Bestimmung der Körperdiskriminante.

Die im vorigen Abschnitte vollständig durchgeführte Untersuchung der Fundamentalsysteme für den Bereich einer beliebigen Primzahl p gibt uns nun das Mittel, auch die absoluten Fundamentalsysteme für die ganzen Zahlen des Körpers $K(\alpha)$ genau kennen zu lernen und die Konstitution der Körperdiskriminante, eines der Hauptprobleme der ganzen Theorie, vollständig anzugeben.

Im § 5 des fünften Kapitels wurde gezeigt, daß man in dem Körper $K(\alpha)$ vom n^{ten} Grade durch eine endliche Anzahl von Versuchen stets ein System $(\eta^{(1)}, \eta^{(2)}, \ldots \eta^{(n)})$ von n ganzen algebraischen Zahlen so bestimmen kann, daß alle und nur die ganzen algebraischen Zahlen von $K(\alpha)$ in der Form:

$$(1) \qquad u_1 \eta^{(1)} + u_1 \eta^{(2)} + \cdots + u_n \eta^{(n)}$$

mit ganzzahligen reellen Koeffizienten u_i darstellbar sind. Ein solches System nannten wir ein Fundamentalsystem für den Körper $K(\alpha)$. Wir bewiesen nun a. S. 121, VIII und S. 122 IX, daß ein System $(\eta^{(1)}, \ldots \eta^{(n)})$ dann und nur dann ein Fundamentalsystem ist, wenn es dieselbe Eigenschaft für den Bereich einer jeden reellen Primzahl $p, q, \ldots$ besitzt. Nach dem im vorigen Paragraphen bewiesenen Satze kommt diese letzte Eigenschaft einem System $(\eta^{(i)})$ von ganzen Zahlen dann und nur dann in bezug auf die Primzahl p zu, wenn seine Diskriminante genau durch das über alle Primteiler $\mathfrak{p}_i$ von p erstreckte Produkt:

$$n(\Pi(\mathfrak{p}_i^{\bar{e}_i - 1}))$$

teilbar ist. Da nun genau derselbe für jede der unendlich vielen reellen Primzahlen $p, q, \ldots$ gilt, so folgt jetzt, daß ein System von n ganzen algebraischen Zahlen $(\eta^{(1)}, \eta^{(2)}, \cdots \eta^{(n)})$, dann und nur dann ein absolutes Fundamentalsystem für den Körper $K(\alpha)$, daß also seine Diskriminante:

$$D(\eta^{(1)}, \eta^{(2)}, \ldots \eta^{(n)}) = |\, \eta_k^{(i)} \,|^2$$

dann und nur dann die Körperdiskriminante ist, wenn dieselbe abgesehen vom Vorzeichen gleich

$$(2) \qquad n\Big(\prod_{\mathfrak{p}} \mathfrak{p}^{\bar{e}-1}\Big) = \prod_{(\mathfrak{p})} p^{f(\bar{e}-1)}$$

ist, wo das Produkt über alle unendlich vielen Primteiler $\mathfrak{p}$ des ganzen Körpers $K(\alpha)$ erstreckt wird, und jedesmal p die zu $\mathfrak{p}$ gehörige Primzahl, $\bar{e}$ die Verzweigungsordnung von $\mathfrak{p}$ bedeutet.

Die Diskriminante eines jeden Systems von n linear unabhängigen ganzen algebraischen Zahlen ist eine von Null verschiedene ganze rationale Zahl, und ist also stets gleich dem Produkte einer endlichen Anzahl gleicher oder verschiedener Primteiler $\mathfrak{p}$. Hieraus folgt, daß das obige Produkt (2) auch nur eine endliche Anzahl von Primteilern $\mathfrak{p}$ enthalten, d. h. daß nur für eine endliche Anzahl derselben $\bar{e} > 1$ sein kann. Es ergibt sich also der wichtige Satz:

In jedem Körper $K(\alpha)$ gibt es nur eine endliche Anzahl von Verzweigungsteilern.

Ich nenne nun das über alle Primdivisoren $\mathfrak{p}$ von $K(\alpha)$, oder, was nach der soeben gemachten Bemerkung dasselbe ist, das nur über die Verzweigungsteiler von $K(\alpha)$ erstreckte Produkt

$$(3) \qquad \mathfrak{Z} = \prod \mathfrak{p}^{\bar{e}-1}$$

den Verzweigungsdivisor oder den Verzweigungsteiler von $K(\alpha)$. Dann ergibt sich jetzt das folgende schöne und für die ganze Theorie der algebraischen Zahlen grundlegende Resultat:

Die Körperdiskriminante eines beliebigen Körpers $K(\alpha)$ ist durch die Gleichung

$$(4) \qquad D(\alpha) = \pm\, n(\mathfrak{Z})$$

bis auf das Vorzeichen vollständig bestimmt.

Im allgemeinen enthält der Verzweigungsdivisor $\mathfrak{Z}$ jeden Primteiler $\mathfrak{p}$ in der $(e-1)^{\text{ten}}$ Potenz, wenn e die Ordnung von $\mathfrak{p}$ ist. Nur für diejenigen Primteiler, deren Ordnung durch die zugehörige Primzahl p teilbar ist, ist $\bar{e} > e$. Da die Ordnung e eines Primteilers höchstens gleich n sein kann, so kann $\mathfrak{Z}$ höchstens die Primteiler derjenigen Primzahlen p, welche gleich oder kleiner als n sind, in höherer als der $(e-1)^{\text{ten}}$ Potenz enthalten, aber auch diese nur, wenn dann e durch p teilbar ist. So tritt für einen Körper $K(\alpha)$ stets nur eine ganz kleine Anzahl von solchen höheren Potenzen von Primfaktoren in dem Verzweigungsteiler auf; aber diese kommen auch wirklich vielfach vor, und es erscheint als ein wesentlicher Vorzug der hier auseinandergesetzten Theorie, daß diese hier keine Ausnahmestellung einnehmen, und der Untersuchung auch nicht die geringste Schwierigkeit bieten.

Durch die vorige Untersuchung ist die Körperdiskriminante nur bis auf das Vorzeichen bestimmt worden. Aber auch dieses läßt sich leicht angeben und zwar mit Hilfe einer Methode, welche die volle Analogie zwischen der bis jetzt durchgeführten Untersuchung der Teilbarkeit der algebraischen Zahlen mit den später zu gebenden Betrachtungen über die Größe der algebraischen Zahlen deutlich hervortreten läßt.

Zunächst ist klar, daß alle von Null verschiedenen Diskriminanten in dem Körper $K(\alpha)$ dasselbe Vorzeichen haben, da je zwei sich nur um das Quadrat einer rationalen Zahl, nämlich der Substitutionsdeterminante unterscheiden. Also braucht man nur festzustellen, welches Vorzeichen z. B. das Produkt $d(f(x)) = \Pi(\alpha_i - \alpha_k)^2$ der quadrierten Wurzeldifferenzen der Grundgleichung:

$$f(x) = 0$$

besitzt, welches ja nach (7c) a. S. 105 mit der Diskriminante $D(f(x))$ jener Gleichung durch die Relation:

(5)
$$d(f(x)) = (-1)^{\frac{n(n-1)}{2}} D(f(x))$$

zusammenhängt.

Ist nun:

(6)
$$f(x) = f_1(x) f_2(x) \ldots f_h(x)$$

die Zerlegung der Funktion $f(x)$ in ihre reellen irreduktiblen Faktoren, d. h. in ihre reellen Linearfaktoren, bzw. in die reellen Faktoren zweiten Grades:

(6a)
$$(x - (a - bi))(x - (a + bi)) = x^2 - 2ax + (a^2 + b^2),$$

deren Linearfaktoren immer je zwei konjugierten komplexen Wurzeln entsprechen, so ergibt sich aus der Gleichung (6), wenn man auf beiden Seiten zu den quadrierten Wurzeldifferenzen übergeht*):

(7)
$$d(f(x)) = \prod_i d(f_i) \cdot \prod_{i>k} R^2(f_i, f_k),$$

und da die reellen Quadratzahlen $R^2(f_i, f_k)$ alle positiv sind, so erhält man durch Übergang zu den Vorzeichen:

$$\operatorname{sgn} d(f(x)) = \prod_i \operatorname{sgn} d(f_i(x)),$$

*) Diese Gleichung folgt entweder direkt, oder aus der entsprechenden Diskriminantengleichung in (7) a. S. 60, wenn man dort nach (5) $D(h(x))$, $D(k(x))$ und $D(h(x)k(x))$ durch $d(h(x))$, $d(k(x))$ und $d(h(x)k(x))$ ersetzt und beachtet, daß dann das Vorzeichen $(-1)^{\alpha\beta}$ fortfällt.

wenn allgemein sgn (a) das Vorzeichen der Zahl a bedeutet. Nun ist aber für einen reellen Linearfaktor, bzw. für einen irreduktiblen reellen Faktor zweiten Grades:

$$d(x-\alpha)=\alpha^2, \qquad d\big((x-(a-bi))\,(x-(a+bi))\big)=(2bi)^2=-4b^2,$$

d. h. ihre Vorzeichen sind bzw. positiv und negativ. Ist also allgemein der irreduktible Faktor $f_i(x)$ vom Grade $\mathfrak{f}_i$, wo $\mathfrak{f}_i$ gleich 1 oder gleich 2 sein kann, so ist

$$\operatorname{sgn} d(f_i(x))=(-1)^{\mathfrak{f}_i-1},$$

und hieraus folgt sofort, wenn man noch beachtet, daß offenbar

$$\mathfrak{f}_1+\mathfrak{f}_2+\cdots+\mathfrak{f}_h=n$$

ist:

(8) $$\operatorname{sgn} d(f(x))=\prod(-1)^{\mathfrak{f}_i-1}=(-1)^{n-h}.$$

Die sämtlichen Diskriminanten der Körpers $K(\alpha)$ sind also positiv oder negativ, je nachdem die Differenz $n-h$ aus dem Grade des Körpers und der Anzahl h der irreduktiblen reellen Faktoren der Grundgleichung gerade oder ungerade ist.

Hierdurch ergibt sich also für die Körperdiskriminante $D(\alpha)$ die folgende auch dem Vorzeichen nach bestimmte Darstellung:

(9) $$D(\alpha)=(-1)^{n-h}\,n(\mathfrak{Z})$$

§ 6. Die Ideale $J(\mathfrak{d})$ des Körpers $K(\alpha)$. Die Fundamentalsysteme für ein Ideal und ihre Diskriminanten.

Die Fundamentalaufgabe für alle Teilbarkeitsfragen in der Theorie der algebraischen Zahlen hatte ich bereits am Anfang des achten Kapitels einfach formuliert; mit Hilfe der soeben durchgeführten Betrachtungen kann sie jetzt ohne Schwierigkeit gelöst werden. Ich sprach diese Aufgabe folgendermaßen aus:

Es sei:

$$\mathfrak{d}=\mathfrak{p}^h\mathfrak{q}^k\mathfrak{r}^l\ldots\mathfrak{t}^m$$

ein beliebiger algebraischer Divisor des Körpers $K(\alpha)$; es sollen alle Vielfachen von $\mathfrak{d}$ innerhalb $K(\alpha)$ gefunden werden.

Ist speziell $\mathfrak{d}=1$, so sind alle Multipla von $\mathfrak{d}$ die sämtlichen ganzen algebraischen Zahlen von $K(\alpha)$; wir haben bewiesen, daß sie alle durch ein Fundamentalsystem $(\xi^{(1)},\cdots\xi^{(n)})$ homogen und ganzzahlig darstellbar sind, welches durch eine endliche Anzahl von Versuchen gefunden werden kann, und dessen Diskriminante $(-1)^{n-h}n(\mathfrak{Z})$ wir im vorigen Abschnitte genau bestimmt haben. Genau die ent-

sprechenden Resultate gelten nun für den Bereich aller Vielfachen von $\mathfrak{d}$.

Alle Multipla von $\mathfrak{d}$ bilden einen durch diesen Divisor vollständig charakterisierten Bereich, welcher durch $\mathfrak{J}(\mathfrak{d})$ bezeichnet, und falls einmal ein Name erwünscht sein sollte, nach Dedekind das zu $\mathfrak{d}$ gehörige Ideal genannt werden soll.

Für die dem Bereiche $\mathfrak{J}(\mathfrak{d})$ zugehörigen Multipla von $\mathfrak{d}$ bestehen dann offenbar die folgenden Sätze:

1. Sind $\zeta^{(1)}, \dots \zeta^{(r)}$ Multipla von $\mathfrak{d}$, so ist auch jede Zahl

$$\eta = u_1 \zeta^{(1)} + u_2 \zeta^{(2)} + \cdots + u_r \zeta^{(r)}$$

ein Vielfaches von $\mathfrak{d}$, falls die Koeffizienten u_i ganze rationale Zahlen sind.

2. Jede Zahl η des Körpers $K(\alpha)$ kann mit einer solchen ganzen rationalen Zahl g multipliziert werden, daß das Produkt:

$$\zeta = g\eta$$

ein Multiplum von $\mathfrak{d}$ wird, also dem Bereiche $\mathfrak{J}(\mathfrak{d})$ angehört.

Ist nämlich η kein Multiplum von $\mathfrak{d}$, ist also

$$\frac{\eta}{\mathfrak{d}} = \frac{\mathfrak{z}}{\mathfrak{n}}$$

in der reduzierten Form noch nicht ein ganzer Divisor, und ist g die kleinste ganze rationale Zahl, welche durch den reduzierten Nenner $\mathfrak{n}$ von $\frac{\eta}{\mathfrak{d}}$ teilbar ist, so ist $g\eta$ durch $\mathfrak{d}$ teilbar und gehört also dem Bereiche $\mathfrak{J}(\mathfrak{d})$ an.

3. Aus dem vorigen Satze folgt, daß man stets ein System von n linear unabhängigen Vielfachen von $\mathfrak{d}$ in dem Körper $K(\alpha)$ finden kann.

Ist nämlich $(\eta^{(1)}, \dots \eta^{(n)})$ irgend ein System von n linear unabhängigen Zahlen von $K(\alpha)$, dessen Diskriminante $D(\eta^{(i)})$ also nicht Null ist, und sind nicht alle seine Elemente Multipla von $\mathfrak{d}$, so kann man sie mit solchen ganzen Zahlen $g_1, \dots g_n$ multiplizieren, daß die n Zahlen $\zeta^{(i)} = g_i \eta^{(i)}$ alle $\mathfrak{d}$ enthalten, und da die Determinante:

$$|\zeta_i^{(1)}, \dots \zeta_i^{(n)}| = |g_1 \eta_i^{(1)}, g_2 \eta_i^{(2)}, \dots g_n \eta_i^{(n)}| = g_1 g_2 \cdots g_n |\eta_i^{(1)}, \dots \eta_i^{(n)}|$$

offenbar ebenfalls von Null verschieden ist, so ist unsere Behauptung bewiesen.

Ist nun $(\zeta^{(1)}, \zeta^{(2)}, \dots \zeta^{(n)})$ irgend ein System von Vielfachen von $\mathfrak{d}$ mit nicht verschwindender Diskriminante, so ist jede Zahl ζ von $K(\alpha)$ auf eine einzige Weise in der Form:

$$\zeta = u_1 \zeta^{(1)} + \cdots + u_n \zeta^{(n)}$$

mit rationalen Koeffizienten darstellbar, und ζ ist sicher ebenfalls ein Multiplum von $\mathfrak{d}$, wenn alle Koeffizienten u_i ganze Zahlen sind. Dagegen kann ζ auch durch $\mathfrak{d}$ teilbar sein, wenn nicht alle u_i ganze Zahlen sind, aber man beweist genau ebenso wie a. S. 112—115 die Richtigkeit des folgenden Satzes:

Man kann für einen beliebigen Divisor $\mathfrak{d}$ stets **ein Fundamentalsystem** $(\xi^{(1)}, \ldots \xi^{(n)})$, d. h. ein System von n solchen Vielfachen von $\mathfrak{d}$ finden, daß jedes Multiplum ξ auf eine einzige Weise in der Form:

$$\xi = u_1 \xi^{(1)} + \cdots + u_n \xi^{(n}$$

mit **ganzzahligen** Koeffizienten darstellbar ist.

Beim Beweise dieses Satzes können wir den Divisor $\mathfrak{d}$ als ganz annehmen; denn ist $\mathfrak{d}$ gebrochen, und g eine solche ganze rationale Zahl, daß

$$\mathfrak{d}_0 = g\mathfrak{d}$$

ein ganzer Divisor ist, und ist dann:

$$\xi^{(1)}, \quad \xi^{(2)}, \ldots \xi^{(n)}$$

ein Fundamentalsystem für den ganzen Divisor $\mathfrak{d}_0$, so ist offenbar

$$\frac{\xi^{(1)}}{g}, \quad \frac{\xi^{(2)}}{g}, \ldots \frac{\xi^{(n)}}{g}$$

ein Fundamentalsystem für den gebrochenen Divisor $\frac{\mathfrak{d}_0}{g} = \mathfrak{d}$; denn eine Zahl ξ enthält ja dann und nur dann den Divisor $\mathfrak{d}_0$, wenn $\frac{\xi}{g}$ den Teiler $\frac{\mathfrak{d}_0}{g}$ besitzt.

Ist nun $\mathfrak{d}$ ein beliebiger ganzer Teiler, und ist $(\xi^{(1)}, \xi^{(2)}, \ldots \xi^{(n)})$ ein linear unabhängiges System von n ganzen algebraischen durch $\mathfrak{d}$ teilbaren Zahlen, so beweist man genau wie a. S. 112 den Satz:

Eine Zahl:

$$(1) \qquad \xi = \frac{v_1 \xi^{(1)} + v_2 \xi^{(2)} + \cdots + v_n \xi^{(n)}}{d}$$

kann nur dann ein Multiplum von $\mathfrak{d}$ sein, wenn bei ihrer Darstellung durch das System $(\xi^{(1)}, \xi^{(2)}, \ldots \xi^{(n)})$ der Nenner d gleich der Diskriminante des Systems $(\xi^{(1)}, \ldots \xi^{(n)})$ ist.

Es sei nun s eine der Zahlen $1, 2, \ldots n$; ich betrachte dann ebenso wie a. a. O. alle diejenigen Multipla von $\mathfrak{d}$:

(1a) $$\gamma^{(s)} = \frac{v_1 \xi^{(1)} + \cdots + v_s \xi^{(s)}}{d},$$

in deren Zähler die Koeffizienten nicht negativ und höchstens gleich d sind; unter diesen sei

(1b) $$\beta^{(s)} = \frac{v_1^{(s)} \xi^{(1)} + \cdots + v_s^{(s)} \xi^{(s)}}{d}$$

diejenige oder eine von denen, bei welchen der Koeffizient $v_s^{(s)}$ von $\xi^{(s)}$ möglichst klein, aber nicht Null ist. Dann beweist man genau wie a. S. 114 daß für jede andere Zahl $\gamma^{(s)}$ der entsprechende Koeffizient v_s durch diesen kleinsten Koeffizienten $v_s^{(s)}$ teilbar sein muß. Sind also wieder die n Zahlen:

(2) $$\begin{aligned} \beta^{(1)} &= \frac{v_1^{(1)} \xi^{(1)}}{d}, \\ \beta^{(2)} &= \frac{v_1^{(2)} \xi^{(1)} + v_2^{(2)} \xi^{(2)}}{d}, \\ \beta^{(3)} &= \frac{v_1^{(3)} \xi^{(1)} + v_2^{(3)} \xi^{(2)} + v_3^{(3)} \xi^{(3)}}{d}, \\ &\vdots \\ \beta^{(n)} &= \frac{v_1^{(n)} \xi^{(1)} + v_2^{(n)} \xi^{(2)} + \cdots + v_n^{(n)} \xi^{(n)}}{d} \end{aligned}$$

ein vollständiges System von n Vielfachen von $\mathfrak{b}$, in welchen bzw. die Koeffizienten $v_1^{(1)}, v_2^{(2)}, \ldots v_n^{(n)}$ positiv und möglichst klein sind, so beweist man wörtlich ebenso, wie a. S. 115, daß alle und nur die Multipla von $\mathfrak{b}$ auf eine einzige Weise in der Form

(3) $$u_1 \beta^{(1)} + \cdots + u_n \beta^{(n)}$$

mit ganzzahligen Koeffizienten darstellbar sind, daß also diese n Zahlen (2) wirklich ein Fundamentalsystem für den Divisor $\mathfrak{b}$ bilden.

Jedes andere Fundamentalsystem $(\gamma^{(1)}, \ldots \gamma^{(n)})$ für denselben Divisor geht aus einem solchen, etwa aus dem soeben gefundenen $(\beta^{(1)}, \ldots \beta^{(n)})$ durch eine ganzzahlige Substitution

(4) $$\gamma^{(i)} = \sum_k c_{ik} \beta^{(k)}$$

hervor, deren Determinante $|c_{ik}| = \pm 1$ ist.

Dies folgt ohne jede Änderung aus dem für die absoluten Fundamentalsysteme a. S. 116—117 geführten Beweise; und durch Übergang zu den Diskriminanten ergibt sich auch hier aus (4) die Gleichung:

(5) $$d(\gamma^{(1)}, \ldots \gamma^{(n)}) = |c_{ik}|^2 \cdot d(\beta^{(1)}, \ldots \beta^{(n)}).$$

Da das System der n Vielfachen $\gamma^{(i)}$ von $\mathfrak{d}$ dann und nur dann ein Fundamentalsystem für diesen Divisor ist, wenn die ganzzahlige Determinante $|c_{ik}| = \pm 1$ ist, so gilt auch hier der Satz:

Ein System von n Vielfachen von $\mathfrak{d}$ ist dann und nur dann ein Fundamentalsystem für $\mathfrak{d}$, wenn seine Diskriminante möglichst klein ist.

Unter Benutzung des am Schlusse von § 4 hergeleiteten Resultates ist es nun leicht, die s. g. Fundamentaldiskriminante für einen Divisor $\mathfrak{d}$, d. h. die Diskriminante des zu $\mathfrak{d}$ gehörigen Fundamentalsystemes zu bestimmen. Es sei nämlich p irgend eine reelle Primzahl, welche wieder der Einfachheit wegen innerhalb $K(\alpha)$ nur die drei voneinander verschiedenen Primfaktoren $\mathfrak{p}_1$, $\mathfrak{p}_2$, $\mathfrak{p}_3$, jeden einzelnen aber ev. auch mehr als einmal enthalten möge. Ferner sei

(6) $$\mathfrak{d}_p = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\mathfrak{p}_3^{r_3}$$

das Produkt der in $\mathfrak{d}$ enthaltenen Potenzen von $\mathfrak{p}_1$, $\mathfrak{p}_2$ und $\mathfrak{p}_3$; dann sind die Exponenten r_i im allgemeinen gleich Null und nur dann von Null verschieden, wenn der bezügliche Primteiler $\mathfrak{p}_i$ wirklich in $\mathfrak{d}$ vorkommt. Ist dann $(\gamma^{(1)}, \gamma^{(2)}, \ldots \gamma^{(n)})$ ein Fundamentalsystem für den Divisor $\mathfrak{d}$, so ist dasselbe System auch ein Fundamentalsystem für das in $\mathfrak{d}$ enthaltene Produkt $\mathfrak{d}_p = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\mathfrak{p}_3^{r_3}$; denn einmal sind in der Form

(7) $$u_1\gamma^{(1)} + u_2\gamma^{(2)} + \cdots + u_n\gamma^{(n)}$$

mit ganzen p-adischen Koeffizienten nur Multipla von $\mathfrak{d}_p$ enthalten, weil ja alle Elemente $\gamma^{(i)}$ durch $\mathfrak{d}$, also auch durch $\mathfrak{d}_p$ teilbar sind. Wäre andererseits auch nur eine solche Zahl mit gebrochenen p-adischen Koeffizienten

(7a) $$\frac{v_1\gamma^{(1)} + v_2\gamma^{(2)} + \cdots + v_n\gamma^{(n)}}{p}$$

durch $\mathfrak{d}_p$ teilbar, so zeigt man genau wie a. S. 121 Mitte, daß dann auch ihr nullter Näherungswert, d. h. die gewöhnliche algebraische Zahl:

(7b) $$\beta_0 = \frac{v_1^{(0)}\gamma^{(1)} + v_2^{(0)}\gamma^{(2)} + \cdots + v_n^{(0)}\gamma^{(n)}}{p}$$

durch $\mathfrak{d}_p$ divisibel sein muß, weil der fortgelassene Teil nach (7) sicher ein Multiplum von $\mathfrak{d}_p$ ist. Da aber dieser Quotient β_0 alle nicht in p enthaltenen Primteiler von $\mathfrak{d}$ ebenso oft enthält, als $\mathfrak{d}$ selbst, und da soeben bewiesen wurde, daß dasselbe auch für $\mathfrak{p}_1^{r_1}$, $\mathfrak{p}_2^{r_2}$ und $\mathfrak{p}_3^{r_3}$ gilt, so wäre dieser Quotient eine algebraische durch $\mathfrak{d}$ teilbare Zahl; das System $(\gamma^{(1)}, \ldots \gamma^{(n)})$ wäre also entgegen unserer Annahme noch kein Fundamentalsystem für $\mathfrak{d}$; damit ist unsere Behauptung bewiesen.

Wir wissen aber nach dem Satze (13) a. S. 233, welche Potenz von p die Diskriminante eines Fundamentalsystems für einen Divisor $\mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\mathfrak{p}_3^{r_3}$ enthält; da nun dieselbe Potenz von p in der Diskriminante von $(\gamma^{(1)}, \ldots \gamma^{(n)})$ auftreten muß, und da dasselbe für eine jede reelle Primzahl gilt, so ergibt sich die wichtige Gleichung:

$$(8) \qquad D(\mathfrak{d}) = \pm \prod_{(\mathfrak{p})} D(\mathfrak{p}^r),$$

wo sich das Produkt rechts auf alle unendlich vielen Primteiler $\mathfrak{p}$ von $K(\alpha)$ erstreckt, und wo $\mathfrak{p}^r$ jedesmal diejenige Potenz von $\mathfrak{p}$ bedeutet welche in $\mathfrak{d}$ enthalten ist. Nach dem a. S. 228 (13a) und (13b) bewiesenen Satze besteht endlich die Gleichung:

$$(8a) \qquad D(\mathfrak{p}^r) = n((\mathfrak{p}^r)^2)\, n(\mathfrak{p}^{\bar{e}-1}),$$

also ergibt die Substitution dieses Wertes in (8):

$$D(\mathfrak{p}^r) = n\Big(\big(\prod_{\mathfrak{p}} \mathfrak{p}^r\big)^2\Big) \cdot n\Big(\prod_{\mathfrak{p}} \mathfrak{p}^{\bar{e}-1}\Big);$$

oder da nach unserer Definition:

$$\prod \mathfrak{p}^r = \mathfrak{d},$$
$$\prod \mathfrak{p}^{\bar{e}-1} = \mathfrak{Z}$$

ist, weil ja jeder Exponent r angibt, wie oft der zugehörige Divisor $\mathfrak{p}$ in $\mathfrak{d}$ enthalten ist, so folgt endlich bei Berücksichtigung des auch hier auftretenden Vorzeichens die Fundamentalgleichung:

$$(9) \qquad D(\mathfrak{d}) = (-1)^{n-f}\, n(\mathfrak{d}^2 \mathfrak{Z}).$$

§ 7. Charakteristische Eigenschaften der Fundamentalsysteme für einen Divisor.

Das soeben gefundene Resultat liefert leicht eine notwendige und hinreichende Bedingung dafür, daß ein vorgelegtes System:

$$(1) \qquad (\xi^{(1)}, \xi^{(2)}, \ldots \xi^{(n)})$$

ein Fundamentalsystem für ein Ideal $I(\mathfrak{D})$ ist, und läßt uns, falls dies der Fall sein sollte, auch sofort den Divisor $\mathfrak{D}$ erkennen, für welchen die n Zahlen (1) ein Fundamentalsystem bilden. Es gilt nämlich der folgende merkwürdige Satz:

Ist $(\xi^{(1)}, \xi^{(2)}, \ldots \xi^{(n)})$ ein beliebiges System von ganzen oder gebrochenen algebraischen Zahlen, und

(1a) $$\mathfrak{D} = (\xi^{(1)}, \xi^{(2)}, \ldots \xi^{(n)})$$

der größte gemeinsame Teiler seiner n Elemente, so ist dieses System dann und nur dann ein Fundamentalsystem für einen Divisor, wenn die Gleichung besteht:

(1b) $$d(\xi^{(i)}) = |\xi_k^{(i)}|^2 = \pm n(\mathfrak{D}^2 \mathfrak{Z}),$$

und zwar ist in diesem Falle jener Divisor genau gleich $\mathfrak{D}$.

In der Tat, ist der Divisor $\mathfrak{D} = (\xi^{(1)}, \xi^{(2)}, \ldots \xi^{(n)})$ der größte gemeinsame Teiler der n Elemente $\xi^{(i)}$, so sind offenbar alle algebraischen Zahlen:

$$w = u_1 \xi^{(1)} + \cdots + u_n \xi^{(n)}$$

mit ganzzahligen Koeffizienten u_i Multipla von $\mathfrak{D}$, und zwar ist $\mathfrak{D}$ der **größte** gemeinsame Teiler aller dieser unendlich vielen Zahlen w, denn man kann ja die u_k stets so wählen, daß das zugehörige w einen beliebigen Primteiler $\mathfrak{p}$ genau so oft enthält, als $\mathfrak{D}$ selbst; ist nämlich $\xi^{(i)}$ ein Element jenes Systemes, welches genau durch die in $\mathfrak{D}$ enthaltene Potenz von $\mathfrak{p}$ teilbar ist, so setze man $u_i = 1$ und alle anderen $u_l = 0$. Ist also $(\xi^{(1)}, \ldots \xi^{(n)})$ überhaupt ein Fundamentalsystem für einen Divisor, so muß dieser gleich $\mathfrak{D}$ sein.

Es sei nun $(\eta^{(1)}, \ldots \eta^{(n)})$ ein Fundamentalsystem für diesen Divisor $\mathfrak{D}$, so ist nach dem im vorigen Paragraphen bewiesenen Satze (9):

$$|\eta_k^{(i)}|^2 = \pm n(\mathfrak{D}^2 \mathfrak{Z}).$$

Da ferner alle n Zahlen $\xi^{(i)}$ auch $\mathfrak{D}$ enthalten, also durch das System $(\eta^{(1)}, \ldots \eta^{(n)})$ darstellbar sind, so bestehen die n Gleichungen mit ganzzahligen Koeffizienten:

$$\xi^{(i)} = \sum_k c_{ik} \eta^{(k)},$$

d. h. es ist:

(1c) $$d(\xi^{(i)}) = |c_{ik}|^2 \cdot d(\eta^{(k)}) = \pm |c_{ik}|^2 \cdot n(\mathfrak{D}^2 \mathfrak{Z}).$$

Dann und nur dann, wenn $|c_{ik}|^2 = 1$ ist, ist auch umgekehrt das System $(\eta^{(k)})$ durch $(\xi^{(i)})$ ganzzahlig ausdrückbar, nur dann ist also $(\xi^{(1)}, \ldots \xi^{(n)})$ ein Fundamentalsystem für den Divisor $\mathfrak{D}$; und da dann (1c) in (1b) übergeht, so ist damit der verlangte Beweis erbracht.

Ich will jetzt einen anderen Ausdruck für die notwendige und hinreichende Bedingung dafür angeben, daß ein System $(\xi^{(1)}, \xi^{(2)}, \ldots \xi^{(n)})$ ein Fundamentalsystem für einen Divisor ist; zu diesem Zwecke schreibe ich die obige Gleichung (1b) in einer anderen, aber völlig äquivalenten Form: Es seien nämlich $\mathfrak{D}_p$, $\mathfrak{Z}_p$ und $d(\xi^{(1)} \ldots \xi^{(n)})_p$ diejenigen Potenzen der zu p gehörigen Primteiler bzw. von p selbst, welche in $\mathfrak{D}$, $\mathfrak{Z}$

und $d(\xi^{(1)}, \ldots \xi^{(n)})$ enthalten sind. Ziehen wir dann aus der Gleichung (1b) links und rechts den auf die Primzahl p gehörigen Teil heraus, so ergibt sich die speziellere Gleichung:

$$(1\text{d}) \qquad d(\xi^{(1)}, \ldots \xi^{(n)})_p = n(\mathfrak{D}_p^2 \mathfrak{Z}_p);$$

da aber das über alle Primzahlen p erstreckte Produkt der beiden Seiten dieser Gleichung wieder die vorige Gleichung (1b) ergibt, so sind beide Bedingungen einander äquivalent. Wir können also das jetzt erlangte Resultat folgendermaßen aussprechen:

Ein System $(\xi^{(1)}, \ldots \xi^{(n)})$ ist dann und nur dann ein Fundamentalsystem für die Multipla eines Divisors $\mathfrak{D}$, wenn dasselbe für den Bereich einer jeden Primzahl p ein Fundamentalsystem für die Multipla des zugehörigen Divisors $\mathfrak{D}_p$ ist. Ist dies umgekehrt der Fall, und ist für den Bereich einer jeden Primzahl p $\mathfrak{D}_p$ derjenige Divisor, für welchen $(\xi^{(i)})$ ein Fundamentalsystem ist, so ist der zu diesem Systeme gehörige Divisor $\mathfrak{D}$ gleich dem über alle reellen Primzahlen p erstreckten Produkte:

$$(2) \qquad \mathfrak{D} = \prod_{(p)} \mathfrak{D}_p.$$

Da man den zu einem Fundamentalsysteme $(\xi^{(1)}, \ldots \xi^{(n)})$ zugehörigen Divisor $\mathfrak{D}_p$, wie jetzt gezeigt werden wird, sehr leicht bestimmen kann, so liefert die Gleichung (2) ein höchst einfaches Mittel, den zu einem Fundamentalsystem gehörigen Divisor $\mathfrak{D}$ zu finden.

Es sei nämlich $(\xi^{(i)})$ ein Fundamentalsystem für die Multipla eines Divisors $\mathfrak{D}$ und es sei wieder wie a. S. 241:

$$(3) \qquad \mathfrak{D}_p = \mathfrak{p}_1^{r_1} \mathfrak{p}_2^{r_2} \mathfrak{p}_3^{r_3}$$

der zu einer beliebigen Primzahl

$$(4) \qquad p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \mathfrak{p}_3^{e_3}$$

gehörige Divisor von $\mathfrak{D}$. Dann ist dieses System $(\xi^{(i)})$ dann und nur dann ein Fundamentalsystem für die Multipla von $\mathfrak{D}_p$, wenn es für den Bereich von p äquivalent ist einem Systeme:

$$\gamma^{(1)}, \ldots \gamma^{(\lambda)}; \quad \delta^{(1)}, \ldots \delta^{(\mu)}; \quad \varepsilon^{(1)} \ldots \varepsilon^{(\nu)},$$

dessen drei Teile $(\gamma^{(i)})$, $(\delta^{(k)})$, $(\varepsilon^{(l)})$ bzw. Fundamentalsysteme für die Multipla von $\mathfrak{p}_1^{r_1}$, $\mathfrak{p}_2^{r_2}$, $\mathfrak{p}_3^{r_3}$ sind, und die wieder so gewählt werden können, daß die zu $\mathfrak{p}_2$ und $\mathfrak{p}_3$ gehörigen Entwicklungen der Zahlen $(\gamma^{(i)})$ gleich Null sind usw. Ich will das aus $(\gamma^{(1)}, \ldots \gamma^{(\lambda)})$ und seinen λ für den Bereich von $\mathfrak{p}_1$ Konjugierten gebildete System:

$$(5)\qquad (\Gamma^{(1)}_{r_1}) = \begin{pmatrix} \gamma^{(1)}_1, & \ldots & \gamma^{(\lambda)}_1 \\ \vdots & & \\ \gamma^{(1)}_\lambda, & \ldots & \gamma^{(\lambda)}_\lambda \end{pmatrix}$$

ein **Partialsystem** der r_1^{ten} **Ordnung** nennen, wenn es ein Fundamentalsystem für die Vielfachen von $\mathfrak{p}_1^{r_1}$ ist, und die entsprechende Bezeichnung soll für die anderen Systeme:

$$(5a)\qquad (\Gamma^{(2)}_{r_2}) = (\delta^{(i_2)}_{k_2}),\qquad (\Gamma^{(3)}_{r_3}) = (\varepsilon^{(i_3)}_{k_3})$$

gelten. Dann kann man das bisher erlangte Resultat folgendermaßen aussprechen:

Ein System $(\xi^{(1)}_k, \xi^{(2)}_k, \ldots \xi^{(n)}_k)$ ist dann und nur dann ein Fundamentalsystem für die Multipla eines Divisors, wenn dasselbe für den Bereich einer jeden reellen Primzahl p äquivalent einem Systeme

$$(6)\qquad \begin{pmatrix} \Gamma^{(1)}_{r_1}, & 0, & 0 \\ 0, & \Gamma^{(2)}_{r_2}, & 0 \\ 0, & 0, & \Gamma^{(3)}_{r_3} \end{pmatrix}$$

ist, welches entsprechend den Primfaktoren $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$ von p in Partialsysteme zerfällt. Ist ferner jedesmal r die Ordnung des zu einem Primteiler $\mathfrak{p}$ gehörigen Partialsystems (Γ_r), so ist der zu dem Fundamentalsystem $(\xi^{(i)}_k)$ gehörige Divisor $\mathfrak{D}$ durch das über alle Primteiler $\mathfrak{p}$ erstreckte Produkt:

$$(7)\qquad \mathfrak{D} = \prod_{(\mathfrak{p})} \mathfrak{p}^r$$

eindeutig bestimmt.

Zwei Systeme sind einander für den Bereich einer Primzahl p dann und nur dann äquivalent, wenn sie ineinander durch eine umkehrbare Transformation mit rationalen ganzzahligen p-adischen Koeffizienten übergehen. Alle wesentlichen Eigenschaften in bezug auf ihr Verhalten zu dieser Primzahl p sind äquivalenten Systemen gemeinsam. Hier können daher statt der Fundamentalsysteme $(\xi^{(i)}_k)$ die ihnen äquivalenten zerfallenden Systeme (6) untersucht werden, und für die in ihnen auftretenden Partialsysteme r^{ter} Ordnung (Γ_r) können die ihnen äquivalenten einfachsten derartigen Systeme, z. B. diejenigen betrachtet werden, welche aus den $ef = \lambda$ konjugierten zu einem Systeme

$$(8)\qquad (\eta^i \pi^{r+k}) = (\pi^r, \eta\pi^r, \ldots \eta^{f-1}\pi^r;\ \pi^{r+1}, \eta\pi^{r+1}, \ldots \eta^{f-1}\pi^{r+1};\ \ldots;\ \pi^{r+e-1}, \ldots \eta^{f-1}\pi^{r+e-1})$$
$$\begin{pmatrix} i = 0, 1, \cdots f-1 \\ k = 0, 1, \cdots e-1 \end{pmatrix}$$

gebildet sind; denn dieses geht ja aus dem Fundamentalsysteme (4) a. S. 222 für den Divisor $\mathfrak{p}^0$ durch Multiplikation mit π^r hervor, ist also nach (11) und (11a) a. S. 226 ein Fundamentalsystem für den Divisor $\mathfrak{p}^r$. Bei Einführung dieser reduzierten Fundamentalsysteme statt der allgemeinen werden nun die meisten ihrer sonst ziemlich verborgenen Eigenschaften so evident, daß sie ohne weiteres abgelesen werden können. Dies soll im nächsten Paragraphen an dem interessanten Beispiel der s. g. komplementären Divisoren deutlich gemacht werden.

§ 8. Komplementäre Systeme und komplementäre Divisoren.

Zu einem beliebigen Systeme

(1)
$$(\eta_k^{(i)}) = \begin{pmatrix} \eta_1^{(1)}, & \dots & \eta_1^{(n)} \\ \vdots & & \\ \eta_n^{(1)}, & \dots & \eta_n^{(n)} \end{pmatrix}$$

mit von Null verschiedener Determinante:

(1a)
$$\mathsf{H} = |\eta_k^{(i)}|$$

gehört bekanntlich ein eindeutig bestimmtes, das s. g. reziproke System*):

(2)
$$(\bar\eta_k^{(i)}) = \begin{pmatrix} \bar\eta_1^{(1)}, & \dots & \bar\eta_1^{(n)} \\ \vdots & & \\ \bar\eta_n^{(1)}, & \dots & \bar\eta_n^{(n)} \end{pmatrix} = \begin{pmatrix} \frac{\mathsf{H}_1^{(1)}}{\mathsf{H}}, & \dots & \frac{\mathsf{H}_n^{(1)}}{\mathsf{H}} \\ \vdots & & \\ \frac{\mathsf{H}_1^{(n)}}{\mathsf{H}}, & \dots & \frac{\mathsf{H}_n^{(n)}}{\mathsf{H}} \end{pmatrix},$$

in welchem jedes Element

(2a)
$$\bar\eta_k^{(i)} = \frac{\mathsf{H}_i^{(k)}}{\mathsf{H}}$$

gleich der zu $\eta_i^{(k)}$ (nicht zu $\eta_k^{(i)}$) gehörigen Unterdeterminante $\mathsf{H}_i^{(k)}$ von (1) dividiert durch die Determinante ist.

Aus der Natur dieser beiden Systeme folgen nun bekanntlich sofort die n^2 Gleichungen:

(3)
$$\overline{H}_i V_l = \bar\eta_i^{(1)} \eta_1^{(l)} + \bar\eta_i^{(2)} \eta_2^{(l)} + \dots + \bar\eta_i^{(n)} \eta_n^{(l)} = \delta_i^{(l)},$$

wo das symbolische Produkt $\overline{H}_i V_l$ die Summe der aus den Elementen $(\bar\eta_i^{(1)}, \dots \bar\eta_i^{(n)})$ der i^{ten} Horizontalreihe $\overline{H}_i$ von (2) und den entsprechenden

*) Die wenigen allein für diesen Paragraphen nötigen Hülfssätze aus der Lehre von den Determinanten sind hier nur kurz bewiesen. Sie finden sich ausführlich dargestellt z. B. in den Vorlesungen über die Theorie der Determinanten von Kronecker, XX. Vorlesung.

Elementen der l^{ten} Vertikalreihe $V_l = (\eta_1^{(l)}, \ldots \eta_n^{(l)})$ von (1) gebildeten Produkte bedeutet und $\delta_i^{(l)}$ gleich Null oder Eins ist, jenachdem $i \gtrless l$ oder $i = l$ ist.

Nach der bekannten Definition für das Produkt zweier Systeme können diese n^2 Gleichungen durch die eine Systemgleichung:

$$(3\text{a}) \qquad (\bar{\eta}_k^{(i)})\,(\eta_k^{(i)}) = (\bar{H}_i\,V_l) = (\delta_k^{(i)}) = (1)$$

vollständig ersetzt werden, in welcher das System $(\delta_k^{(i)}) = (1)$ das s. g. **Einheitssystem**, d. h. das Diagonalsystem bedeutet, dessen sämtliche Diagonalelemente gleich Eins, alle übrigen aber Null sind.

Aus der Gleichung (3a) folgt nun leicht die allgemeinere Relation:

$$(3\text{b}) \qquad (\bar{\eta}_k^{(i)})\,(\eta_k^{(i)}) = (\eta_k^{(i)})\,(\bar{\eta}_k^{(i)}) = (1),$$

d. h. jedes System ist mit seinem reziproken Systeme vertauschbar.

Ist also $(\bar{\eta}_k^{(i)})$ reziprok zu $(\eta_k^{(i)})$, so ist auch umgekehrt $(\eta_k^{(i)})$ zu $(\bar{\eta}_k^{(i)})$ reziprok.

Durch Übergang zu den Determinanten ergibt sich ferner aus (3a)

$$(3\text{c}) \qquad |\bar{\eta}_k^{(i)}|\,|\eta_k^{(i)}| = 1,$$

d. h. die Determinanten reziproker Systeme sind reziproke Zahlen.

Ist

$$(4) \qquad (\zeta_k^{(i)}) = (\eta_k^{(i)})\,(a_k^{(i)})$$

ein System, welches aus $(\eta_k^{(i)})$ durch hintere Multiplikation mit einem Systeme $(a_k^{(i)})$ von nicht verschwindender Determinante hervorgeht, so ergiebt sich für das reziproke System $(\bar{\zeta}_k^{(i)})$ die Darstellung:

$$(4\text{a}) \qquad (\bar{\zeta}_k^{(i)}) = (\bar{a}_k^{(i)})\,(\bar{\eta}_k^{(i)}),$$

denn in der Tat besteht ja für dieses System die Gleichung:

$$(4\text{b}) \qquad (\bar{\zeta}_k^{(i)})\,(\zeta_k^{(i)}) = (\bar{a}_k^{(i)})\,(\bar{\eta}_k^{(i)})\,(\eta_k^{(i)})\,(a_k^{(i)}) = (\bar{a}_k^{(i)})\,(1)\,(a_k^{(i)}) = (1$$

Das reziproke System eines Produktes aus zwei (oder auch aus mehr als zwei) Faktoren ist gleich dem Produkte der reziproken Systeme der Faktoren, aber in umgekehrter Reihenfolge.

Vertauscht man in einem Systeme $(\eta_k^{(i)})$ irgend zwei Vertikalreihen, etwa V_1 und V_2 und zugleich in dem reziproken Systeme $(\bar{\eta}_k^{(i)})$ die beiden entsprechenden Horizontalreihen $\bar{H}_1$ und $\bar{H}_1$, so bestehen offenbar für die so sich ergebenden Systeme ebenfalls die

Gleichungen (3a), da bei dieser Vertauschung nur die Reihenfolge jener Gleichungen geändert wird; die so geänderten Systeme sind also ebenfalls reziprok.

Anstatt der reziproken Systeme will ich nun die von ihnen nicht wesentlich verschiedenen s. g. komplementären Systeme betrachten, welche mit jenen durch die folgende Definition zusammenhängen:

Das zu einem Systeme $(\eta_k^{(i)})$ gehörige komplementäre System $(\breve{\eta}_k^{(i)})$ geht aus dem reziproken Systeme $(\bar{\eta}_k^{(i)})$ durch Vertauschung der Horizontalreihen mit den Vertikalreihen hervor.

Nach (2a) ist also allgemein:

$$\breve{\eta}_k^{(i)} = \bar{\eta}_i^{(k)} = \frac{\mathsf{H}_k^{(i)}}{\mathsf{H}}, \tag{5}$$

d. h. $\breve{\eta}_k^{(i)}$ ist gleich der zu dem entsprechenden Elemente $\eta_k^{(i)}$ gehörigen Unterdeterminante $\mathsf{H}_k^{(i)}$, dividiert durch die Determinante.

Übertragen wir nun die für das reziproke System gefundenen Resultate auf das komplementäre System, so ergeben sich die folgenden Sätze:

Zu jedem Systeme $(\eta_k^{(i)})$ von nicht verschwindender Determinante H gehört ein einziges komplementäres System

$$(\breve{\eta}_k^{(i)}) = \left(\frac{\mathsf{H}_k^{(i)}}{\mathsf{H}}\right), \tag{5}$$

dessen Elemente mit denjenigen von $(\eta_k^{(i)})$ durch die n^2 Gleichungen

$$\breve{V}_i V_l = \sum_{k=1}^{n} \breve{\eta}_k^{(i)} \eta_k^{(l)} = \breve{\eta}_1^{(i)} \eta_1^{(l)} + \cdots + \breve{\eta}_n^{(i)} \eta_n^{(l)} = \delta_{il}, \tag{5a}$$

oder auch durch die entsprechenden Gleichungen für die Horizontalreihen:

$$\breve{H}_i H_l = \sum_k \breve{\eta}_i^{(k)} \eta_l^{(k)} = \delta_{il} \tag{5b}$$

zusammenhängen. Ist $(\breve{\eta}_k^{(i)})$ komplementär zu $(\eta_k^{(i)})$, so ist auch umgekehrt das zweite System komplementär zum ersten.

Komplementäre Systeme haben reziproke Determinanten.

Vertauscht man endlich in zwei komplementären Systemen dieselben beiden Parallelreihen miteinander, etwa H_1 und H_2 und $\breve{H}_1$ und $\breve{H}_2$, so bleiben die entstehenden Systeme komplementär.

Ist

$$(\xi_k^{(i)}) = (\eta_k^{(i)})\,(a_k^{(i)}) \tag{6}$$

das Produkt zweier Systeme von nicht verschwindenden Determinanten, so ergab sich durch Übergang zu den reziproken Systemen:

(6a) $$(\bar{\zeta}_k^{(i)}) = (\bar{a}_k^{(i)})\,(\bar{\eta}_k^{(i)}).$$

Vertauscht man nun links und rechts in den reziproken Systemen die Zeilen und die Kolonnen, wodurch sie in die komplementären Systeme übergehen, so gehen die n^2 aus (3) folgenden Kompositionsgleichungen:

(6b) $$\bar{\zeta}_i^{(l)} = \sum_k \bar{a}_i^{(k)}\,\bar{\eta}_k^{(l)} = H_i(\bar{a})\,V_l(\bar{\eta})$$

über in die folgenden:

(6c) $$\breve{\zeta}_l^{(i)} = \sum_k \breve{a}_k^{(i)}\,\breve{\eta}_l^{(k)},$$

oder wenn man noch beiderseits die Indexbezeichnungen i und l vertauscht:

(6d) $$\breve{\zeta}_i^{(l)} = \sum_k \breve{\eta}_i^{(k)}\,\breve{a}_k^{(l)} = H_i(\breve{\eta})\,V_l(\breve{a}),$$

d. h. es besteht die Systemgleichung:

(6e) $$(\breve{\zeta}_k^{(i)}) = (\breve{\eta}_k^{(i)})\,(\breve{a}_k^{(i)}).$$

Das zu einem Produkte von zwei (oder mehreren) Systemen komplementäre System ist gleich dem Produkte der Komplemente der Faktoren in ungeänderter Reihenfolge.

Ich nehme jetzt speziell an, das System $(\eta_k^{(i)})$ zerfalle folgendermaßen in Teilsysteme:

(7) $$(\eta_k^{(i)}) = \begin{pmatrix} \mathsf{H}^{(1)}, & 0 \\ 0, & \mathsf{H}^{(2)} \end{pmatrix} = \left\{\begin{matrix} \eta_1^{(1)} \dots \eta_1^{(\lambda)} & 0 & \dots 0 \\ \vdots & & \\ \eta_\lambda^{(1)} \dots \eta_\lambda^{(\lambda)} & 0 & \dots 0 \\ 0 \quad \dots \quad 0 & \eta_{\lambda+1}^{(\lambda+1)} & \dots \eta_{\lambda+1}^{(n)} \\ \vdots \qquad\quad \vdots & \vdots & \\ 0 \qquad\quad 0 & \eta_n^{(\lambda+1)} & \dots \eta_n^{(n)} \end{matrix}\right\},$$

und es sei seine Determinante

(7a) $$|\eta_k^{(i)}| = |\mathsf{H}^{(1)}| \cdot |\mathsf{H}^{(2)}|$$

von Null verschieden. Dann besitzen auch die Teilsysteme $(\mathsf{H}^{(1)})$ und $(\mathsf{H}^{(2)})$ von Null verschiedene Determinanten. Also gehört zu jedem dieser beiden kleineren Systeme je ein komplementäres System $(\breve{\mathsf{H}}^{(1)})$ und $(\breve{\mathsf{H}}^{(2)})$ bzw. von der λ^{ten} und der $(n-\lambda)^{\text{ten}}$ Ordnung, und man

zeigt leicht, daß sich das zu $(\eta_k^{(i)})$ komplementäre System folgendermaßen aus diesen zusammensetzt:

$$(7\text{b})\qquad (\breve{\eta}_k^{(i)}) = \begin{pmatrix} \breve{\mathsf{H}}^{(1)}, & 0 \\ 0, & \breve{\mathsf{H}}^{(2)} \end{pmatrix} = \begin{pmatrix} \breve{\eta}_1^{(1)} \ldots \breve{\eta}_1^{(\lambda)} & 0 & \ldots 0 \\ \vdots & & \\ \breve{\eta}_\lambda^{(1)} \ldots \breve{\eta}_\lambda^{(\lambda)} & 0 & \ldots 0 \\ 0 \quad \ldots 0 & \breve{\eta}_{\lambda+1}^{(\lambda+1)} & \ldots \breve{\eta}_{\lambda+1}^{(n)} \\ \vdots \qquad \vdots & \vdots & \\ 0 \qquad 0 & \breve{\eta}_n^{(\lambda+1)} & \ldots \breve{\eta}_n^{(n)} \end{pmatrix}.$$

In der Tat bestehen ja die für die komplementären Systeme charakteristischen Gleichungen:

$$(7\text{c})\qquad V_i(\eta)\, V_l(\breve{\eta}) = \delta_{il}$$

für die beiden Systeme (7) und (7b); denn gehören i und l entweder beide der Reihe $(1, 2, \ldots \lambda)$ oder beide der Reihe $(\lambda + 1, \ldots n)$ an, so ist die Gleichung (7c) erfüllt, weil $\mathsf{H}^{(1)}$ und $\breve{\mathsf{H}}^{(1)}$, oder weil $\mathsf{H}^{(2)}$ und $\breve{\mathsf{H}}^{(2)}$ komplementär sind; gehört dagegen von den Indizes i und l der eine der ersten, der andere der zweiten Zahlenreihe an, so ist

$$V_i(\eta)\, V_l(\breve{\eta}) = 0,$$

da in jedem der links stehenden n Produkte mindestens ein Faktor Null ist. Da genau der entsprechende Satz besteht, wenn $(\eta_k^{(i)})$ in mehr als zwei Teilsysteme zerfällt, so ergibt sich das folgende Resultat:

Ist das System $(\eta_k^{(i)})$ von nicht verschwindender Determinante aus Teilsystemen zusammengesetzt, so ist das komplementäre System aus den komplementären Teilsystemen in gleicher Weise zusammengesetzt.

Ich benutze diese Resultate jetzt zur Untersuchung der algebraischen Systeme: Es sei $(\eta^{(1)}, \eta^{(2)}, \ldots \eta^{(n)})$ ein beliebiges algebraisches System des Körpers $K(\alpha)$, und $(\eta_k^{(i)})$ sei die aus den n^2 zu $(\eta^{(1)}, \ldots \eta^{(n)})$ konjugierten algebraischen Zahlen gebildete Matrix, deren Horizontalreihen H_i also die zu jenem Systeme in dem Körper $K(\alpha_i)$ konjugierten Zahlen enthalten.

Ist dann, wie wir annehmen wollen, die Determinante $\mathsf{H} = |\eta_k^{(i)}|$ von Null verschieden, so gehört zu dem Systeme $(\eta_k^{(i)})$ ein eindeutig bestimmtes komplementäres System:

$$(8)\qquad (\breve{\eta}_k^{(i)}) = \left(\frac{\mathsf{H}_k^{(i)}}{\mathsf{H}}\right),$$

dessen Elemente $(\breve{\eta}_k^{(i)})$ also ebenfalls rationale Funktionen von $(\alpha_1, \alpha_2, \ldots \alpha_n)$ sind. Ich zeige zunächst leicht, daß auch hier die Elemente einer, etwa der ersten Horizontalreihe $\breve{H}_1$ rationale Funktionen von α_1 allein, d. h.

Zahlen des Körpers $K(\alpha_1)$ sind, und daß die Elemente der anderen Horizontalreihen die konjugierten zu den entsprechenden Elementen von $\breve{H}_1$ für die Körper $K(\alpha_2), \ldots K(\alpha_n)$ sind. Vertauscht man nämlich irgend zwei Wurzeln α_i und α_k der Grundgleichung miteinander, so vertauschen sich in dem Systeme $(\eta_k^{(i)})$ nur die beiden zugehörigen Horizontalreihen H_i und H_k, während die übrigen ungeändert bleiben; nach dem soeben bewiesenen Satze a. S. 248 unten vertauschen sich dann in dem komplementären Systeme dieselben Horizontalreihen $\breve{H}_i$ und $\breve{H}_k$. Hieraus folgt also daß z. B. die Elemente $(\breve{\eta}_1^{(1)}, \ldots \breve{\eta}_1^{(n)})$ der ersten Horizontalreihe H_1 von $(\breve{\eta}_k^{(i)})$ solche rationale Funktionen von $(\alpha_1, \alpha_2, \ldots \alpha_n)$ sind, daß sie ungeändert bleiben, wenn man zwei Wurzeln α_i und α_k der Reihe $(\alpha_2, \ldots \alpha_n)$ permutiert; sie sind also symmetrische Funktionen von $\alpha_2, \ldots \alpha_n$, d. h. sie sind rational durch α_1 allein ausdrückbar. Da aber endlich z. B. H_1 in $\breve{H}_i$ übergeht, wenn α_1 mit α_i vertauscht wird, so folgt, daß z. B. die Elemente $(\eta_i^{(1)}, \ldots \eta_i^{(n)})$ von $\breve{H}_i$ dieselben rationalen Funktionen von α_i sind, wie es die entsprechenden Elemente der Reihe $\breve{H}_1$ von α_1 waren. Damit ist der verlangte Beweis erbracht.

Zu jedem algebraischen Systeme $(\eta^{(1)}, \ldots \eta^{(n)})$ des Körpers $K(\alpha)$ von nicht verschwindender Determinante gehört also ein eindeutig bestimmtes komplementäres System $(\breve{\eta}^{(1)}, \breve{\eta}^{(2)}, \ldots \breve{\eta}^{(n)})$ desselben Körpers.

Sind $(\eta^{(i)})$ und $(\breve{\eta}^{(i)})$ zwei komplementäre Systeme, $(\eta_k^{(i)})$ und $(\breve{\eta}_k^{(i)})$ die zugehörigen komplementären Matrizen, so stehen diese nach (5a) in der Beziehung zueinander, daß allgemein die n^2 Gleichungen:

$$V^{(i)}\breve{V}^{(l)} = \sum_{k=1}^{n} \eta_k^{(i)} \breve{\eta}_k^{(l)} = \delta_{il} \tag{9}$$

erfüllt sind, und durch diese ist das komplementäre System eindeutig bestimmt. Für die algebraischen Systeme sind nun die in einer Vertikalreihe $V^{(i)}$ bzw. $\breve{V}^{(i)}$ stehenden Zahlen alle die bzw. zu $\eta^{(i)}$ und $\breve{\eta}^{(i)}$ konjugierten algebraischen Zahlen.

Ich will nun im folgenden stets die Summe der n zu einer algebraischen Zahl n^{ter} Ordnung ζ konjugierten Zahlen $\zeta_1, \zeta_2, \ldots \zeta_n$ nach Dedekind die Spur von ζ nennen und sie durch

$$S(\zeta) = \zeta_1 + \zeta_2 + \cdots + \zeta_n \tag{9a}$$

bezeichnen. Dann kann ich jene n^2 charakteristischen Gleichungen (9) durch die einfacheren:

$$S(\eta^{(i)}\breve{\eta}^{(l)}) = \delta_{il} \tag{9b}$$

ersetzen. Diese Gleichungen will ich nun mit Hilfe der folgenden Überlegung in eine einzige zusammenziehen:

Ist $(\eta^{(1)}, \dots \eta^{(n)})$ ein beliebiges algebraisches System, so will ich die Linearform mit unbestimmten Koeffizienten:

$$w = u_1\eta^{(1)} + u_2\eta^{(2)} + \cdots + u_n\eta^{(n)} \tag{10}$$

die zu jenem Systeme gehörige Linearform nennen. Zu jeder solchen Linearform w gehören dann n konjugierte Formen:

$$w_i = u_1\eta_i^{(1)} + \cdots + u_n\eta_i^{(n)}, \qquad (i = 1, 2, \cdots n) \tag{10a}$$

welche aus w dadurch hervorgehen, daß α der Reihe nach durch $\alpha_1, \alpha_2, \dots \alpha_n$ ersetzt wird.

Es seien nun $(\eta^{(i)})$ und $(\breve{\eta}^{(i)})$ zwei komplementäre Systeme,

$$w = \sum_i u_i\eta^{(i)}, \qquad \breve{w} = \sum_i \breve{u}_i\breve{\eta}^{(i)} \tag{11}$$

die zugehörigen Linearformen, welche komplementäre Linearformen genannt werden sollen. Bildet man dann das Produkt:

$$w\breve{w} = \sum_i \sum_l u_i\breve{u}_l\eta^{(i)}\breve{\eta}^{(l)} \tag{11a}$$

und addiert die n konjugierten Produkte $w_i\breve{w}_i$, so folgt aus den Gleichungen (9b) sofort die merkwürdige und einfache Beziehung:

$$S(w\breve{w}) = \sum_i \sum_l u_i\breve{u}_l\delta_{il} = u_1\breve{u}_1 + u_2\breve{u}_2 + \cdots + u_n\breve{u}_n, \tag{11b}$$

und umgekehrt ergeben sich die n^2 Gleichungen (9b) für jede Indexkombination (i, l), indem man in (11b) $u_i = \breve{u}_l = 1$, alle anderen Unbestimmten gleich Null setzt. So erhält man den Satz:

> Zwei algebraische Linearformen w und $\breve{w}$ sind dann und nur dann komplementär, wenn die Spur $S(w\breve{w})$ ihres Produktes gleich der s. g. Einheitsform $\sum u_i\breve{u}_i$ ist.

Ich gebe nun einige elementare Eigenschaften der komplementären algebraischen Systeme an, welche uns den Beweis des gleich aufzustellenden Fundamentalsatzes wesentlich erleichtern werden. Es sei $(\eta^{(1)}, \dots \eta^{(n)})$ ein beliebiges algebraisches System von nicht verschwindender Determinante. Ist dann $(\zeta^{(1)}, \dots \zeta^{(n)})$ irgend ein anderes algebraisches System desselben Körpers, so hängen seine Elemente mit denen des Systemes $(\eta^{(i)})$ durch eine Substitution:

$$\zeta^{(i)} = \sum_{k=1}^{n} a_k^{(i)}\eta^{(k)} \tag{12}$$

mit rationalen Koeffizienten zusammen, deren Determinante $|a_k^{(i)}|$ von Null verschieden ist, wenn, was wir annehmen wollen, auch das System $(\zeta^{(i)})$ eine von Null verschiedene Determinante besitzt. Aus den Gleichungen (12) folgt aber die Systemgleichung:

(12a) $$(\zeta_k^{(i)}) = (\eta_k^{(i)})\,(a_k^{(i)}).$$

Geht man hier zu den komplementären Systemen über, so besteht nach (6e) die Gleichung:

(12b) $$(\breve{\zeta}_k^{(i)}) = (\breve{\eta}_k^{(i)})\,(\breve{a}_k^{(i)}),$$

und aus ihr folgt also, daß die Elemente $(\breve{\zeta}^{(i)})$ und $(\breve{\eta}^{(i)})$ der beiden komplementären Systeme durch die Gleichungen:

(12c) $$\breve{\zeta}^{(i)} = \sum \breve{a}_k^{(i)}\,\breve{\eta}^{(k)}$$

zusammenhängen. Es ergibt sich also der Satz:

Geht ein algebraisches System $(\zeta^{(i)})$ aus einem anderen $(\eta^{(i)})$ durch die Substitution $(a_k^{(i)})$ hervor, so hängt das komplementäre System $(\breve{\zeta}^{(i)})$ mit dem komplementären $(\breve{\eta}^{(i)})$ durch die komplementäre Substitution $(\breve{a}_k^{(i)})$ zusammen.

Ist speziell das Substitutionssystem $(a_k^{(i)})$ ganzzahlig und unimodular, so gilt dasselbe auch von dem komplementären Systeme $(\breve{a}_k^{(i)})$, da ja der einzige bei letzterem auftretende Nenner die Determinante $|a_k^{(i)}|$ ist. Das entsprechende ist für den Bereich einer Primzahl p der Fall, wenn die Elemente $a_k^{(i)}$ modulo p ganz, d. h. ganze p-adische Zahlen und die Determinante eine Einheit modulo p ist. Nennen wir zwei Systeme $(\eta^{(i)})$ und $(\zeta^{(i)})$ a b s o l u t o d e r f ü r d e n B e r e i c h v o n p ä q u i v a l e n t, wenn jedes von ihnen mit dem anderen durch eine absolut oder modulo p ganzzahlige Substitution zusammenhängt, so können wir das soeben gefundene Resultat so aussprechen:

(12d) Sind zwei Systeme $(\eta^{(i)})$ und $(\zeta^{(i)})$ absolut bzw. für den Bereich von p äquivalent, so gilt das gleiche für die beiden komplementären Systeme $(\breve{\eta}^{(i)})$ und $(\breve{\zeta}^{(i)})$.

Sind $(\eta^{(i)})$ und $(\breve{\eta}^{(i)})$ zwei komplementäre Systeme eines Körpers $K(\alpha)$ und ist ξ eine beliebige Zahl desselben Körpers, so sind

(13) $$(\xi\eta^{(1)}, \ldots \xi\eta^{(n)}) \quad \text{und} \quad \left(\frac{\breve{\eta}^{(1)}}{\xi}, \ldots \frac{\breve{\eta}^{(n)}}{\xi}\right)$$

ebenfalls komplementäre Systeme.

Sind nämlich w und $\breve{w}$ die zu den ersten komplementären Systemen

gehörigen Linearformen, so entsprechen den beiden letzten die Formen ξw und $\frac{\breve{w}}{\xi}$; es ist somit wirklich:

$$(14)\qquad S\left((\xi w)\cdot\left(\frac{\breve{w}}{\xi}\right)\right)=S(w\breve{w})=\sum u_i\breve{u}_i.$$

Es sei nun speziell η eine beliebige algebraische Zahl ν^{ter} Ordnung, und

$$(15)\qquad g(x)=x^\nu+a_{\nu-1}x^{\nu-1}+a_{\nu-2}x^{\nu-2}+\cdots+a_0=0$$

sei die irreduktible Gleichung, der die ν konjugierten Zahlen $\eta_1,\eta_2,\ldots\eta_\nu$ genügen. Es soll das zu

$$(16)\qquad (1,\ \eta,\ \eta^2,\ \ldots\ \eta^{\nu-1})$$

komplementäre System $(\breve{\eta}^{(0)},\breve{\eta}^{(1)},\ldots\breve{\eta}^{(\nu-1)})$ bestimmt werden.

Entwickelt man den Quotienten:

$$(17)\qquad \frac{g(x)}{(x-\eta)\,g'(\eta)}=\frac{1}{g'(\eta)}\cdot\frac{g(x)-g(\eta)}{x-\eta}=\breve{\eta}^{(0)}+\breve{\eta}^{(1)}x+\cdots+\breve{\eta}^{(\nu-1)}x^{\nu-1}$$

nach Potenzen von x, so erhält man eine ganze Funktion vom $(\nu-1)^{\text{ten}}$ Grade in x, deren Koeffizienten rationale Funktionen von η d. h. Zahlen des Körpers $K(\eta)$ sind, und zwar ist, wie die Ausführung der Division lehrt:

$$(17\text{a})\qquad \begin{aligned}\breve{\eta}^{(0)}&=\frac{\eta^{\nu-1}+a_{\nu-1}\eta^{\nu-2}+a_{\nu-2}\eta^{\nu-3}+\cdots+a_1}{g'(\eta)},\\ \breve{\eta}^{(1)}&=\frac{\eta^{\nu-2}+a_{\nu-1}\eta^{\nu-3}+\cdots+a_2}{g'(\eta)},\\ &\ \vdots\\ \breve{\eta}^{(\nu-1)}&=\frac{1}{g'(\eta)};\end{aligned}$$

dann bilden diese ν Zahlen $(\breve{\eta}^{(i)})$ das komplementäre System zu (η^i). Bildet man nämlich die Summe:

$$(18)\qquad \begin{aligned}&S((u_0+u_1\eta+\cdots+u_{\nu-1}\eta^{\nu-1})(\breve{\eta}^{(0)}+\breve{\eta}^{(1)}x+\cdots+\breve{\eta}^{(\nu-1)}x^{\nu-1}))\\ &\quad=S\left((u_0+u_1\eta+\cdots+u_{\nu-1}\eta^{\nu-1})\frac{g(x)}{(x-\eta)\,g'(\eta)}\right),\end{aligned}$$

so ist sie eine ganze Funktion vom $(\nu-1)^{\text{ten}}$ Grade in x, welche nach der Lagrangeschen Interpolationsformel gleich:

$$(18\text{a})\qquad u_0+u_1x+\cdots+u_{\nu-1}x^{\nu-1}$$

ist. In der Tat ist ja die Summe:

$$(18\text{b})\qquad \sum_{i=1}^{n} (u_0 + u_1\eta_i + \cdots + u_{\nu-1}\eta^{\nu-1}) \frac{g(x)}{(x-\eta_i)\,g'(\eta_i)}$$

gleich der Funktion (18a), weil sie eine ganze Funktion des $(\nu-1)^{\text{ten}}$ Grades in x ist, welche für die ν Werte $x = \eta_i$ mit jener Funktion übereinstimmt. Setzt man also in der so bewiesenen Identität:

$$S((u_0 + u_1\eta + \cdots + u_{\nu-1}\eta^{\nu-1})(\breve{\eta}^{(0)} + \breve{\eta}^{(1)}x + \cdots + \breve{\eta}^{(\nu-1)}x^{\nu-1}))$$
$$= u_0 + u_1 x + \cdots + u_{\nu-1}x^{\nu-1}$$

die Koeffizienten aller Produkte $u_i x^l$ auf beiden Seiten einander gleich, so folgen die ν^2 Gleichungen

$$(18\text{c})\qquad S(\eta^i \breve{\eta}^{(l)}) = \delta_{il},$$

welche aussagen, daß die beiden Systeme (η^i) und $(\breve{\eta}^{(i)})$ in der Tat komplementär sind.

Aus den Gleichungen (17a) folgt, daß das System

$$(19)\qquad (\breve{\eta}^{(0)}, \breve{\eta}^{(1)}, \ldots \breve{\eta}^{(\nu-1)})$$

aus dem Systeme:

$$(19\text{a})\qquad \left(\frac{\eta^{\nu-1}}{g'(\eta)}, \frac{\eta^{(\nu-2)}}{g'(\eta)}, \ldots \frac{1}{g'(\eta)}\right)$$

durch die lineare Substitution:

$$(19\text{b})\qquad (a_k^{(i)}) = \begin{pmatrix} 1, & a_{\nu-1}, & a_{\nu-2}, & \ldots & a_1 \\ 0, & 1, & a_{\nu-1}, & \ldots & a_2 \\ 0, & 0, & 1, & \ldots & a_3 \\ \vdots & & & & \\ 0, & 0, & 0, & \ldots & 1 \end{pmatrix}$$

mit der Determinante $|a_k^{(i)}| = 1$ hervorgeht. Ist also η algebraisch ganz, so sind die Gleichungskoeffizienten a_i ebenfalls ganze Zahlen; in diesem Falle sind somit die beiden Systeme (19) und (19a) äquivalent, weil sie durch die unimodulare ganzzahlige Substitution (19b) zusammenhängen. Es gilt also der Satz:

Ist η eine beliebige ganze algebraische Zahl ν^{ter} Ordnung, welche der Gleichung $g(x) = 0$ genügt, so ist das zu

$$(1, \eta, \ldots \eta^{\nu-1})$$

komplementäre System äquivalent dem Systeme

$$(19\text{c})\qquad \left(\frac{1}{g'(\eta)}, \frac{\eta}{g'(\eta)}, \ldots \frac{\eta^{\nu-1}}{g'(\eta)}\right).$$

Ich wende dieses Resultat an, um das System zu bestimmen, welches zu dem a. S. 245, (8) aufgestellten Partialsysteme r^{ter} Ordnung:

$$(20)\qquad \eta^i \pi^{k+r} \qquad \begin{pmatrix} i = 0, 1, \cdots f-1 \\ k = 0, 1, \cdots e-1 \end{pmatrix}$$

komplementär ist. Da sich dieses von einem Partialsysteme nullter Ordnung:

$$(20\text{a})\qquad \eta^i \pi^k \qquad \begin{pmatrix} i = 0, 1, \cdots f-1 \\ k = 0, 1, \cdots e-1 \end{pmatrix}$$

nur durch den gemeinsamen Faktor π^r unterscheidet, so genügt es, zu diesem Systeme das komplementäre zu bestimmen, da sich aus ihm das komplementäre System zu (20) nach (13) einfach durch Division mit π^r ergibt.

Es seien nun:

$$(21)\qquad \begin{aligned} \varphi(x) &= x^f + a_{f-1}x^{f-1} + \cdots + a_0 = (x-\eta_1)\,(x-\eta_2)\cdots(x-\eta_f) = 0, \\ \psi(y, \eta_i) &= y^e + pC_{e-1}y^{e-1} + \cdots + pC_0 = (y-\pi_1^{(i)})(y-\pi_2^{(i)})\cdots(y-\pi_e^{(i)}) = 0 \end{aligned}$$

die Gleichungen, denen die f zu η und die ef zu $\pi^{(i)}$ konjugierten Zahlen für $i = 1, 2, \cdots f$ genügen. Bildet man nun wieder die beiden Quotienten:

$$(21\text{a})\qquad \begin{aligned} \frac{\varphi(x)}{(x-\eta)\,\varphi'(\eta)} &= \breve{\eta}^{(0)} + \breve{\eta}^{(1)}x + \cdots + \breve{\eta}^{(f-1)}x^{f-1}, \\ \frac{\psi(y, \eta)}{(y-\pi)\,\psi'(\pi)} &= \breve{\pi}^{(0)} + \breve{\pi}^{(1)}y + \cdots + \breve{\pi}^{(e-1)}y^{e-1}, \end{aligned}$$

wo die Koeffizienten $\breve{\eta}^{(i)}$ und $\breve{\pi}^{(k)}$ die aus (17a) folgende Bedeutung haben:

$$(22)\qquad \begin{aligned} \breve{\eta}^{(i)} &= \frac{\eta^{f-i-1} + a_{f-1}\eta^{f-i-2} + \cdots + a_{i+1}}{\varphi'(\eta)}, \\ \breve{\pi}^{(k)} &= \frac{\pi^{e-k-1} + pC_{e-1}\pi^{e-k-2} + \cdots + pC_{k+1}}{\psi'(\pi, \eta)}, \end{aligned}$$

so behaupte ich, daß das aus diesen Zahlen gebildete System:

$$(22\text{a})\qquad (\breve{\eta}^{(i)}\breve{\pi}^{(k)}) \qquad \begin{pmatrix} i = 0, 1, \cdots f-1 \\ k = 0, 1, \cdots e-1 \end{pmatrix}$$

das zu $(\eta^i \pi^k)$ komplementäre System ist.

Der Beweis dieses Satzes ergibt sich wieder sofort aus der Identität:

$$(23)\qquad \begin{aligned} \sum_{l=1}^{f} \sum_{m=1}^{e} &(u_0 + u_1\eta_l + \cdots + u_{f-1}\eta_l^{f-1})\,(v_0 + v_1\pi_m^{(l)} + \cdots + v_{e-1}\pi_m^{(l)e-1}) \\ &\times \frac{\varphi(x)}{(x-\eta_l)\,\varphi'(\eta_l)}\,\frac{\psi(y, \eta_l)}{(y-\pi_m^{(l)})\,\psi'(\pi_m^{(l)}, \eta_l)} \\ &= (u_0 + u_1x + \cdots + u_{f-1}x^{f-1})\,(v_0 + v_1y + \cdots + v_{e-1}y^{e-1}), \end{aligned}$$

welche auch hier nichts anderes als ein spezieller Fall der Lagrangeschen Interpolationsformel ist; denn die ganze Funktion auf der rechten Seite, welche in x vom $(f-1)^{\text{ten}}$, in y vom $(e-1)^{\text{ten}}$ Grade ist, stimmt ja für die ef Wertsysteme $(x = \eta_l,\ y = \pi_m^{(l)})$ mit der Summe auf der linken Seite überein, ist also mit dieser identisch. Ersetzt man aber in der Summe links die beiden letzten Faktoren jedesmal durch ihre Entwicklungen (21a) und multipliziert dann auf beiden Seiten aus, so geht jene Gleichung über in:

$$(23\text{a})\qquad S\left(\left(\sum_{i,k} u_i v_k \eta^i \pi^k\right)\left(\sum_{i',k'} x^{i'} y^{k'} \breve{\eta}^{(i')} \breve{\pi}^{(k')}\right)\right) = \sum_{i,k} u_i v_k x^i y^k,$$

und aus ihr ergeben sich durch Koeffizientenvergleichung die folgenden ef Gleichungen:

$$(23\text{b})\qquad S\left((\eta^i \pi^k)(\breve{\eta}^{(i')} \breve{\pi}^{(k')})\right) = \begin{cases}1\\0\end{cases},$$

je nachdem die beiden Indexsysteme (i, k) und (i', k') gleich oder verschieden sind. Diese Gleichungen sagen aber in der Tat aus, daß die beiden Systeme:

$$(\eta^i \pi^k) \qquad \text{und} \qquad (\breve{\eta}^{(i)} \breve{\pi}^{(k)})$$

komplementär sind. Endlich folgt, wie oben bereits erwähnt wurde, daß zu dem allgemeinen Partialsysteme r^{ter} Ordnung

$$(24)\qquad (\eta^i \pi^{r+k}) \qquad \text{das System} \qquad \left(\frac{\breve{\eta}^{(i)} \breve{\pi}^{(k)}}{\pi^r}\right)$$

komplementär ist.

Das Partialsystem r^{ter} Ordnung $(\eta^i \pi^{r+k})$ war nun, wie wir a. S. 245 (8) bewiesen hatten, ein Fundamentalsystem für alle Multipla von $\mathfrak{p}^r$, wenn $\mathfrak{p}$ der zugehörige Primteiler ist. Es ist nun eine besonders wichtige und merkwürdige Tatsache, daß auch das komplementäre System $\left(\frac{\breve{\eta}^{(i)} \breve{\pi}^{(k)}}{\pi^r}\right)$ ebenfalls ein Fundamentalsystem für die Multipla einer anderen Potenz $\mathfrak{p}^{\breve{r}}$ desselben Primteilers ist, und zwar derjenigen, für welche:

$$(25)\qquad \mathfrak{p}^{r+\breve{r}} = \frac{1}{\mathfrak{p}^{\bar{e}-1}}$$

ist, wo wieder $\bar{e}$ die Verzweigungsordnung von $\mathfrak{p}$ bedeutet.

Ich brauche zu diesem Zwecke nur zu zeigen, daß das zu $(\eta^i \pi^{r+k})$ komplementäre System:

$$\left(\frac{\breve{\eta}^{(i)} \breve{\pi}^{(k)}}{\pi^r}\right)$$

äquivalent dem Partialsysteme

$$(\eta^i \pi^{\breve{r}+k})$$

ist, wo $\breve{r}$ durch die Gleichung (25) definiert ist, daß sich also die ef Elemente jenes komplementären Systemes homogen und linear mit modulo p ganzen Koeffizienten durch diejenigen des Partialsystemes $(\eta^i \pi^{\breve{r}+k})$ darstellen lassen und daß auch das umgekehrte der Fall ist.

Nun folgt aber aus dem Satze (19.c), daß das System

$$(\breve{\eta}^{(0)}, \breve{\eta}^{(1)}, \ldots \breve{\eta}^{(f-1)})$$

äquivalent

$$\left(\frac{1}{\varphi'(\eta)}, \frac{\eta}{\varphi'(\eta)}, \ldots \frac{\eta^{f-1}}{\varphi'(\eta)}\right)$$

ist, d. h. daß die Zahlen $\eta^{(i)}$ homogen linear und ganzzahlig durch die Elemente $\frac{\eta^i}{\varphi'(\eta)}$ darstellbar sind und umgekehrt. Aus demselben Satze folgt auch, daß die Elemente der Systeme:

$$(\breve{\pi}^{(0)}, \breve{\pi}^{(1)}, \ldots \breve{\pi}^{(e-1)}) \quad \text{und} \quad \left(\frac{1}{\psi'(\pi)}, \frac{\pi}{\psi'(\pi)}, \ldots \frac{\pi^{e-1}}{\psi'(\pi)}\right)$$

gegenseitig durch einander homogen, linear und ganzzahlig darstellbar sind, wo hier allerdings die Substitutionskoeffizienten nach (19) und (21) nicht ganze rationale, sondern g a n z e algebraische Zahlen von $K(\eta)$ sind; dies ist aber für das weitere unwesentlich. Hieraus folgt, daß auch jedes Element des Systemes: $(\breve{\eta}^{(i)} \breve{\pi}^{(k)})$ homogen und linear mit ganzzahligen Koeffizienten durch die Elemente des Systemes

$$\left(\frac{\eta^i \pi^k}{\varphi'(\eta)\,\psi'(\pi)}\right)$$

darstellbar ist, und daß auch das Umgekehrte gilt; denn ich brauche ja nur jede der linearen Gleichungen für $\breve{\eta}^{(0)}, \breve{\eta}^{(1)}, \ldots \breve{\eta}^{(f-1)}$ mit jeder Gleichung für $\breve{\pi}^{(0)}, \breve{\pi}^{(1)}, \ldots \breve{\pi}^{(e-1)}$ zu multiplizieren, um jene Gleichungen für alle Produkte $\breve{\eta}^{(i)} \breve{\pi}^{(k)}$ zu erhalten, und das entsprechende für die Umkehrungsgleichungen auszuführen. Dividiert man also noch beide Systeme durch π^r, so folgt, daß die beiden Systeme

$$\left(\frac{\breve{\eta}^{(i)} \breve{\pi}^{(k)}}{\pi^r}\right) \quad \text{und} \quad \left(\frac{\eta^i \pi^{k-r}}{\varphi'(\eta)\,\psi'(\pi)}\right)$$

äquivalent sind; es ist also nur noch zu untersuchen, ob das zweite System ein Partialsystem ist, und falls dies der Fall sein sollte, welches seine Ordnung $\breve{r}$ ist. Nun ist aber $\varphi'(\eta)$ eine Einheit modulo $\mathfrak{p}$, weil η zum Exponenten f gehört, und $\psi'(\pi) = \pi^{\bar{e}-1}\varepsilon$, wo auch ε eine Einheit ist (vgl. S. 219 (9a)). Also ist dieses zweite System äquivalent

$$(\eta^i \pi^{-(r-k+\bar{e}-1)}) = (\eta^i \pi^{\breve{r}+k}),$$

wenn

$$-(r+\bar{e}-1)=\breve{r} \quad \text{also} \quad r+\breve{r}=-(\bar{e}-1)$$

gesetzt wird. Und hieraus in Verbindung mit dem Theorem (12d) folgt also wirklich der Satz:

Ist ein System ein Fundamentalsystem für alle Multipla einer Primteilerpotenz $\mathfrak{p}^r$, so ist das komplementäre System ebenfalls ein Fundamentalsystem für die Multipla einer Potenz $\mathfrak{p}^{\breve{r}}$ desselben Primteilers, und zwar besteht zwischen jenen Potenzen stets die Gleichung:

(26) $$\mathfrak{p}^r \mathfrak{p}^{\breve{r}} = \frac{1}{\mathfrak{p}^{\bar{e}-1}}.$$

Mit Hilfe dieser Resultate beweise ich nun den Fundamentalsatz in der Theorie der komplementären Systeme, welcher folgendermaßen ausgesprochen werden kann:

Ist $(\eta^{(1)}, \eta^{(2)}, \ldots \eta^{(n)})$ ein Fundamentalsystem für alle Multipla eines beliebig gegebenen Divisors $\mathfrak{D}$, so ist das komplementäre System $(\breve{\eta}^{(1)}, \breve{\eta}^{(2)}, \ldots \breve{\eta}^{(n)})$ ebenfalls ein Fundamentalsystem für die Multipla eines anderen, des s. g. komplementären Divisors $\breve{\mathfrak{D}}$. — Je zwei komplementäre Divisoren $\mathfrak{D}$ und $\breve{\mathfrak{D}}$ sind miteinander stets durch die Gleichung:

(27) $$\mathfrak{D}\breve{\mathfrak{D}} = \frac{1}{\mathfrak{Z}}$$

verbunden, wo $\mathfrak{Z}$ den Verzweigungsteiler des Körpers bedeutet.

Die beiden komplementären Systeme $(\eta^{(i)})$ und $(\breve{\eta}^{(i)})$ sind dann und nur dann Fundamentalsysteme bzw. für die beiden komplementären Divisoren $\mathfrak{D}$ und $\breve{\mathfrak{D}}$, wenn dieselben Systeme für den Bereich einer jeden Primzahl p Fundamentalsysteme für die Multipla der auf p bezüglichen Teile $\mathfrak{D}_p$ und $\breve{\mathfrak{D}}_p$ jener komplementären Divisoren sind; diese sind also miteinander durch die Gleichung:

(27a) $$\mathfrak{D}_p \cdot \breve{\mathfrak{D}}_p = \frac{1}{\mathfrak{Z}_p}$$

verbunden, wo $\mathfrak{Z}_p$ den auf p bezüglichen Bestandteil des Verzweigungsteilers bedeutet. Ich brauche hiernach den obigen Satz nur für den Bereich einer reellen Primzahl p zu beweisen.

Es sei also $p=\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\mathfrak{p}_3^{e_3}$ eine beliebige Primzahl, und $(\eta^{(i)})$ sei für den Bereich von p ein Fundamentalsystem für die Multipla des Divisors

$$\mathfrak{D}_p = \mathfrak{p}_1^{r_1}\mathfrak{p}_2^{r_2}\mathfrak{p}_3^{r_3}.$$

Nach dem a. S. 245 bewiesenen Satze (6) ist dies dann und nur dann der Fall, wenn

$$(28)\qquad (\eta_k^{(i)}) \sim \begin{pmatrix} \Gamma_{r_1}^{(1)}, & 0, & 0 \\ 0, & \Gamma_{r_2}^{(2)}, & 0 \\ 0, & 0, & \Gamma_{r_3}^{(3)} \end{pmatrix} \qquad (p)$$

ist, wo allgemein $\Gamma_{r_i}^{(i)}$ das zu $\mathfrak{p}_i^{r_i}$ gehörige Partialsystem der r_i^{ten} Ordnung bedeutet.

Nach dem a. S. 250 Mitte bewiesenen Satze ist aber dann:

$$(28\text{a})\qquad (\breve{\eta}_k^{(i)}) \sim \begin{pmatrix} \breve{\Gamma}^{(1)}, & 0, & 0 \\ 0, & \breve{\Gamma}^{(2)}, & 0 \\ 0, & 0, & \breve{\Gamma}^{(3)} \end{pmatrix} \qquad (p),$$

wo allgemein $\breve{\Gamma}^{(i)}$ das zu $\Gamma_{r_i}^{(i)}$ komplementäre System bedeutet. Da nun nach dem Theoreme (26) jedes solches komplementäre System $\breve{\Gamma}^{(i)}$ ebenfalls einem Partialsysteme $\breve{\Gamma}_{\breve{r}_i}^{(i)}$ äquivalent ist, dessen Ordnung $\breve{r}_i$ mit r_i durch die Gleichung

$$(28\text{b})\qquad r_i + \breve{r}_i = -(\bar{e}_i - 1)$$

zusammenhängt, so ergibt sich unter Voraussetzung der Äquivalenz (28) für das komplementäre System:

$$(28\text{c})\qquad (\breve{\eta}_k^{(i)}) \sim \begin{pmatrix} \breve{\Gamma}_{\breve{r}_1}^{(1)}, & 0, & 0 \\ 0, & \breve{\Gamma}_{\breve{r}_2}^{(2)}, & 0 \\ 0, & 0, & \breve{\Gamma}_{\breve{r}_3}^{(3)} \end{pmatrix} \qquad (p);$$

das rechts, mithin auch das links stehende System ist also ein Fundamentalsystem und zwar für den Divisor

$$\breve{\mathfrak{D}}_p = \mathfrak{p}_1^{\breve{r}_1}\,\mathfrak{p}_2^{\breve{r}_2}\,\mathfrak{p}_3^{\breve{r}_3},$$

dessen Exponenten $\breve{r}_i$ durch die Gleichungen (28b) bestimmt sind. Aus ihnen ergibt sich daher die Gleichung:

$$\mathfrak{D}_p\,\breve{\mathfrak{D}}_p = \mathfrak{p}_1^{r_1+\breve{r}_1}\,\mathfrak{p}_2^{r_2+\breve{r}_2}\,\mathfrak{p}_3^{r_3+\breve{r}_3} = \frac{1}{\mathfrak{p}_1^{\bar{e}_1-1}\,\mathfrak{p}_2^{\bar{e}_2-1}\,\mathfrak{p}_3^{\bar{e}_3-1}} = \frac{1}{\mathfrak{Z}_p},$$

und hierdurch ist die Gleichung (27a) und damit auch unser ganzes Fundamentaltheorem vollständig bewiesen.

Zehntes Kapitel.

Die ganzen algebraischen Zahlen. Die Fundamentalform, die Fundamentalgleichung und die Fundamentaldiskriminante eines Körpers. Die wesentlichen und außerwesentlichen Diskriminantenteiler. Die gemeinsamen außerwesentlichen Diskriminantenteiler.

———

§ 1. Die Fundamentalform, die Fundamentalgleichung und die Fundamentaldiskriminante.

Ich gehe nun zu einer eingehenden Untersuchung der ganzen Zahlen eines Körpers $K(\alpha)$ über; gerade bei der Ergründung der tiefer liegenden Eigenschaften dieser Zahlen wird sich zeigen, wie naturgemäß die hier dargelegte Betrachtung der algebraischen Zahlen ist; stimmen doch die nun abzuleitenden Resultate fast wörtlich mit den entsprechenden Ergebnissen der Kurventheorie überein.

Es sei wieder $K(\alpha)$ ein beliebiger Körper n^{ter} Ordnung, und

$$(1) \qquad (\xi^{(1)}, \xi^{(2)}, \ldots \xi^{(n)})$$

ein beliebiges Fundamentalsystem für seine ganzen algebraischen Zahlen, so daß alle ganzen Zahlen von $K(\alpha)$ durch die zugehörige Linearform:

$$(1\text{a}) \qquad w = u_1 \xi^{(1)} + u_2 \xi^{(2)} + \cdots + u_n \xi^{(n)}$$

auf eine einzige Weise dargestellt werden, wenn man $u_1, u_2, \ldots u_n$ unabhängig voneinander alle rationalen ganzen Zahlen durchlaufen läßt. Aus diesem Grunde nennt man die Linearform (1a) mit unbestimmten Koeffizienten u_i die zu $K(\alpha)$ gehörige Fundamentalform.

Eine andere algebraische Linearform desselben Körpers

$$(1\text{b}) \qquad \overline{w} = v_1 \eta^{(1)} + v_2 \eta^{(2)} + \cdots + v_n \eta^{(n)}$$

ist dann und nur dann gleichfalls eine Fundamentalform, wenn das System $(\eta^{(k)})$ auch ein Fundamentalsystem ist, wenn also seine Elemente

mit denjenigen des Systemes $(\xi^{(i)})$ durch eine unimodulare ganzzahlige Substitution zusammenhängen. Ist dies der Fall, und ist:

$$\eta^{(k)} = \sum_i c_{ki}\,\xi^{(i)} \tag{1c}$$

jene Substitution, so geht durch sie die Form $\bar{w}$ über in:

$$\bar{w} = \sum_k v_k \eta^{(k)} = \sum_{k,i} v_k c_{ki} \xi^{(i)} = \sum_i u_i \xi^{(i)} = w, \tag{1d}$$

wenn in w die Koeffizienten

$$u_i = \sum_k c_{ki} v_k \tag{1e}$$

gesetzt werden, wenn also auf die Koeffizienten u_i die transponierte Substitution zu (1c), d. h. diejenige angewendet wird, in welcher die Horizontal- und Vertikalreihen miteinander vertauscht sind. Da diese ebenfalls unimodular ist, wenn es die ursprüngliche Substitution war, so ergibt sich der Satz:

(1f) Alle Fundamentalformen des Körpers $K(\alpha)$ gehen aus einer von ihnen durch eine beliebige unimodulare ganzzahlige Transformation ihrer Unbestimmten hervor.

Ist allgemeiner $(\zeta^{(1)}, \zeta^{(2)}, \ldots \zeta^{(n)})$ ein Fundamentalsystem des Körpers $K(\alpha)$ für den Bereich einer Primzahl p, so nenne ich die zugehörige Linearform:

$$\bar{w} = v_1\zeta^{(1)} + v_2\zeta^{(2)} + \cdots + v_n\zeta^{(n)} \tag{1g}$$

eine Fundamentalform für den Bereich dieser Primzahl; und da in diesem und nur in diesem Falle das System $(\zeta^{(i)})$ aus dem absoluten Fundamentalsystem $(\xi^{(i)})$ durch eine Substitution (c_{ik}) hervorgeht, deren Koeffizienten modulo p ganze Zahlen sind, und deren Determinante eine Einheit modulo p ist, so ergibt sich genau wie vorher der Satz, daß alle und nur die Fundamentalformen (1g) für den Bereich von p aus einer unter ihnen durch eine beliebige modulo p unimodulare und ganzzahlige Transformation der Unbestimmten $(u_1, u_2, \ldots u_n)$ hervorgehen.

Die n zu einer Fundamentalform konjugierten:

$$\begin{aligned} w_1 &= u_1\xi_1^{(1)} + u_2\xi_1^{(2)} + \cdots + u_n\xi_1^{(n)}, \\ w_2 &= u_1\xi_2^{(1)} + u_2\xi_2^{(2)} + \cdots + u_n\xi_2^{(n)}, \\ &\vdots \\ w_n &= u_1\xi_n^{(1)} + u_2\xi_n^{(2)} + \cdots + u_n\xi_n^{(n)} \end{aligned} \tag{2}$$

sind Fundamentalformen für die n konjugierten Körper

$$K(\alpha_1),\ K(\alpha_2),\ \ldots\ K(\alpha_n);$$

aus ihnen erhält man alle konjugierten ganzen algebraischen Zahlen von $K(\alpha)$ und nur sie, wenn man in (2) den Unbestimmten u_i alle ganzzahligen Werte beilegt.

Die n konjugierten Fundamentalformen genügen für unbestimmte $u_1, \ldots u_n$ einer Gleichung des n^{ten} Grades:

$$(3) \qquad F(w;\, u_1, \ldots u_n) = w^n + U^{(1)} w^{n-1} + \cdots + U^{(n)} = 0,$$

deren Koeffizienten $U^{(1)}, U^{(2)}, \ldots U^{(n)}$ offenbar homogene Funktionen des ersten, zweiten, ... n^{ten} Grades von $u_1, \ldots u_n$ mit ganzzahligen Koeffizienten sind. Legt man hier den Größen u alle möglichen ganzzahligen Werte bei, so erhält man die Gleichungen für alle ganzen Zahlen des Körpers $K(\alpha)$ und nur diese, während man alle Gleichungen jenes Körpers erhalten würde, wenn man für die Unbestimmten u_i überhaupt alle rationalen ganzen oder gebrochenen Zahlen setzen würde. Aus diesem Grunde wird jene Gleichung (3) nach Kronecker die Fundamentalgleichung jenes Körpers genannt. Diese Gleichung ist offenbar im Gebiete der rationalen Zahlen unzerlegbar, d. h. sie zerfällt für unbestimmte u_i nicht in rationale ganzzahlige Faktoren niedrigeren Grades; denn dann würden ja auch alle Gleichungen, denen die Zahlen von $K(\alpha)$ genügen, in gleicher Weise zerfallen, dieser Körper wäre also nicht von der n^{ten} Ordnung.

Die Diskriminante der Fundamentalgleichung (s. S. 105 (7)) oder die Fundamentaldiskriminante:

$$(4) \qquad \mathfrak{D}(u_1, u_2, \ldots u_n) = \prod_{i>k} (w_i - w_k)^2 = \begin{vmatrix} 1, & 1, & \ldots & 1 \\ w_1, & w_2, & \ldots & w_n \\ \vdots & & & \\ w_1^{n-1}, & w_2^{n-1}, & \ldots & w_n^{n-1} \end{vmatrix}^2,$$

d. h. das Quadrat der Differenzen aller konjugierten Fundamentalformen w_i, ist offenbar eine homogene ganzzahlige Funktion des $n(n-1)^{\text{ten}}$ Grades von $u_1, \ldots u_n$, welche alle und nur die Gleichungsdiskriminanten $d(1, \beta, \ldots \beta^{n-1})$ für die ganzen algebraischen Zahlen β des Körpers $K(\alpha)$ darstellt, wenn den u_i alle ganzzahligen Werte beigelegt werden.

Alle diese Gleichungsdiskriminanten enthalten, wie bereits a. S. 117 Ende hervorgehoben wurde, die Körperdiskriminante $D = |\xi_k^{(i)}|^2$ als gemeinsamen Teiler, weil diese ja in jeder Diskriminante einer Basis von ganzen algebraischen Zahlen enthalten ist. Eine einfache Überlegung lehrt aber genauer, daß die Form $\mathfrak{D}(u_1, u_2, \ldots u_n)$ für unbestimmte u_i die Körperdiskriminante D als Zahlenteiler enthalten muß. Bildet man nämlich für unbestimmte u_i die homogenen Formen der nullten, ersten, ... $(n-1)^{\text{ten}}$ Dimension $1, w, w^2, \ldots w^{n-1}$, so besitzen diese

ganze algebraische Zahlkoeffizienten, welche also alle durch das Fundamentalsystem $(\xi^{(1)}, \ldots \xi^{(n)})$ homogen linear und ganzzahlig ausgedrückt werden können. Tut man das, so ergeben sich n Gleichungen von der Form:

$$
(5) \qquad \begin{aligned}
1 &= U_1^{(0)} \xi^{(1)} + U_2^{(0)} \xi^{(2)} + \cdots + U_n^{(0)} \xi^{(n)}, \\
w &= U_1^{(1)} \xi^{(1)} + U_2^{(1)} \xi^{(2)} + \cdots + U_n^{(1)} \xi^{(n)}, \\
&\vdots \\
w^{n-1} &= U_1^{(n-1)} \xi^{(1)} + U_2^{(n-1)} \xi^{(2)} + \cdots + U_n^{(n-1)} \xi^{(n)},
\end{aligned}
$$

in denen jedes $U_k^{(i)}$ eine ganze ganzzahlige homogene Funktion der $u_1, \ldots u_n$ von der i^{ten} Dimension ist. Beachtet man weiter, daß dieselben Gleichungen für die n konjugierten Körper $K(\alpha_i)$ bestehen, so ergibt sich für die Fundamentaldiskriminante (4) die folgende Darstellung:

$$
(5\text{a}) \qquad \mathfrak{D}(u_1, \ldots u_n) = |w_i^{k-1}|^2 = |U_m^{(i)}|^2 \, |\xi_k^{(i)}|^2 = D \cdot |U_m^{(i)}|^2.
$$

Die Diskriminante der Fundamentalgleichung ist also gleich der ganzzahligen Form $|U_m^{(i)}|^2$ multipliziert mit der Körperdiskriminante D.

Hiermit ist aber erst eine untere Grenze für den größten gemeinsamen Teiler aller Gleichungsdiskriminanten von $K(\alpha)$ gegeben, denn die ganzzahlige Form $|U_m^{(i)}|^2$ kann ja für unbestimmte $u_1, \ldots u_n$ sehr wohl noch einen weiteren Zahlenteiler enthalten. Im folgenden Paragraphen soll jene Frage vollständig untersucht und beantwortet werden, und zwar wird sich das grundlegende Resultat ergeben, daß die Diskriminante der Fundamentalgleichung für unbestimmte u_i außer der Körperdiskriminante keinen Zahlenteiler enthält. Jede Gleichungsdiskriminante einer ganzen algebraischen Zahl

$$
\beta = a_1 \xi^{(1)} + \cdots + a_n \xi^{(n)}
$$

des Körpers $K(\alpha)$ läßt sich also folgendermaßen darstellen:

$$
d(1, \beta, \cdots \beta^{n-1}) = D \cdot |A_m^{(i)}|^2,
$$

wo $|A_m^{(i)}|^2$ der Wert ist, den die primitive Form $|U_m^{(i)}|^2$ für $u_i = a_i$ annimmt. Der allen jenen Gleichungsdiskriminanten $d(\beta)$ gemeinsame Zahlenteiler D, welcher also gleich der Körperdiskriminante ist, soll nun nach Kronecker der wesentliche Teiler dieser Diskriminanten genannt werden, während die primitive Form $|U_m^{(i)}|^2$ in (5a) der außerwesentliche Bestandteil der Fundamentaldiskriminante heißen soll; entsprechend soll auch für jede Diskriminante $d(\beta)$ die Zahl $|A_m^{(i)}|^2$ ihr außerwesentlicher Teiler genannt werden.

Während nun der wesentliche Teiler D für alle Diskriminanten $d(\beta)$ derselbe ist, wird der außerwesentliche Teiler $|A_m^{(i)}|^2$ für jede Diskri-

minante einen anderen Wert besitzen; aber obwohl der außerwesentliche Bestandteil $|U_m^{(i)}|^2$ der Körperdiskriminante primitiv, also für unbestimmte u_i durch keine einzige Primzahl p teilbar ist, könnte jene Form doch sehr wohl so beschaffen sein, daß alle ganzen Zahlen $|A_m^{(i)}|^2$, denen sie für beliebige ganzzahlige Werte der Unbestimmten gleich wird, eine und dieselbe Primzahl p als Teiler enthalten. Auch diese zweite Frage wird im § 4 dieses Kapitels sehr einfach gelöst werden, und es zeigt sich, daß im allgemeinen jeder Körper $K(\alpha)$ solche s. g. außerwesentliche Diskriminantenteiler p hat, welche also neben der Körperdiskriminante D in allen Gleichungsdiskriminanten $d(\beta)$ des Körpers enthalten sind, ohne doch in der Diskriminante der Fundamentalgleichung für unbestimmte u_i als Zahlenteiler vorzukommen. — Ich wende mich zuerst zur vollständigen Bestimmung des Zahlenteilers der Körperdiskriminante $\mathfrak{D}(u_1, u_2, \ldots u_n)$.

§ 2. Beweis der Äquivalenz der Körperdiskriminante und der Diskriminante der Fundamentalgleichung.

Es sei nun $\mathfrak{D}$ der Zahlenteiler der Diskriminante einer Fundamentalgleichung für den Körper $K(\alpha)$, so daß also

$$\mathfrak{D}(u_1, \ldots u_n) = \mathfrak{D} \cdot \mathfrak{E}(u_1, \ldots u_n) \tag{1}$$

ist, wo $\mathfrak{E}(u_i)$ eine primitive oder Einheitsform d. h. eine ganzzahlige Form mit teilerfremden Koeffizienten bedeutet. Dann ist $\mathfrak{D}$ sicher ein Vielfaches der Körperdiskriminante D, und es soll jetzt bewiesen werden, daß stets $\mathfrak{D} = D$ sein muß. Ersetzt man die zu (1) gehörige Fundamentalform $\sum u_i \xi^{(i)}$ durch irgend eine andere $\sum v_i \eta^{(i)}$, und ist

$$\bar{\mathfrak{D}}(v_1, \ldots v_n) = \bar{\mathfrak{D}} \bar{\mathfrak{E}}(v_1, \ldots v_n) \tag{1a}$$

die entsprechende Zerlegung ihrer Diskriminante, so muß $\mathfrak{D} = \bar{\mathfrak{D}}$ sein; denn da die beiden Fundamentalformen, also auch die beiden Diskriminanten (1) und (1a) nach (1f.) a. S. 262 durch zwei ganzzahlige Transformationen

$$u_i = \sum_k c_{ik} v_k, \qquad v_i = \sum_k c'_{ik} u_k \tag{1b}$$

ineinander übergehen, so folgt durch die Anwendung der ersten Transformation auf (1), daß $\bar{\mathfrak{D}}$ ein Vielfaches von $\mathfrak{D}$ ist, während die Ausführung der zweiten Transformation in (1a) ergibt, daß $\mathfrak{D}$ ein Multiplum von $\bar{\mathfrak{D}}$ sein muß.

Um nun den Zahlenteiler von $\mathfrak{D}(u_i)$ zu finden, braucht man nur die Potenz einer beliebigen Primzahl p zu bestimmen, welche in $\mathfrak{D}$ enthalten ist. Es werde diese Potenz wieder durch $\mathfrak{D}_p$ bezeichnet, so daß:

(2) $$\mathfrak{D}(u_1, \dots u_n) = \mathfrak{D}_p \cdot \mathfrak{E}_p(u_1, \dots u_n)$$

ist, wo $\mathfrak{E}_p(u_i)$ jetzt eine primitive Form für den Bereich von p, d. h. eine ganzzahlige Form bezeichnet, deren Koeffizienten nur keine Potenz von p als gemeinsamen Teiler enthalten. Ist dann $\sum v_i \eta^{(i)}$ irgend eine andere Fundamentalform für den Bereich von p, so folgt aus den Bemerkungen bei (1g) a. S. 262 genau wie vorher, daß ihre Diskriminante $\overline{\mathfrak{D}}(v_1, \dots v_n)$ genau denselben Teiler $\mathfrak{D}_p$ besitzt wie die Diskriminante (2). Zur Bestimmung dieses Teilers können wir also von vornherein ein beliebiges Fundamentalsystem für den Bereich von p zu Grunde legen.

Es sei nun $K(\alpha_1)$ einer der n konjugierten Körper und

(3) $$w_1 = u_1 \xi_1^{(1)} + \cdots + u_n \xi_1^{(n)}$$

eine Fundamentalform von $K(\alpha_1)$ für den Bereich von p. Ist dann wieder $\mathfrak{p}$ der zu $K(\alpha_1)$ gehörige Primteiler, e seine Ordnung und f sein Grad, so lassen sich alle Zahlen $\xi_1^{(i)}$ nach steigenden Potenzen einer zu $\mathfrak{p}$ gehörigen Primzahl π_1 entwickeln, deren Koeffizienten sämtlich $(p^f - 1)^{\text{te}}$ Einheitswurzeln oder Null sind. Substituiert man diese Reihen in (3) und ordnet dann nach den Potenzen von π_1, so ergibt sich für die Form w_1 eine Entwicklung

(3a) $$w_1 = U_0 + U_1 \pi_1 + U_2 \pi_1^2 + \cdots,$$

deren Koeffizienten U_i homogene Linearformen der (u_i) multipliziert mit $(p^f - 1)^{\text{ten}}$ Einheitswurzeln sind. Zu dieser Form sind nun für den Bereich des Koeffizientenkörpers $K(\eta)$ zunächst die e Formen $w_1, w_2, \dots w_e$ konjugiert, welche aus w_1 dadurch hervorgehen, daß man in ihnen π_1 der Reihe nach durch die $e-1$ zu π_1 für den Bereich von η konjugierten Primzahlen $\pi_2, \pi_3, \dots \pi_e$ ersetzt, welche der zugehörigen Eisensteinschen Gleichung:

(4) $$\psi(x, \eta) = x^e + p c_{e-1} x^{e-1} + \cdots + p c_0 = 0$$

genügen. Für sie ist allgemein:

(5) $$w_i = U_0 + U_1 \pi_i + U_2 \pi_i^2 + \cdots \qquad (i = 1, 2, \cdots e).$$

Ersetzt man in diesen e konjugierten Reihen überall die in den Koeffizienten U_k auftretenden Einheitswurzeln durch ihre $(p)^{\text{ten}}, (p^2)^{\text{ten}} \dots (p^{f-1})^{\text{ten}}$

Potenzen, so erhält man alle $ef = \lambda$ für den Bereich dieses Primteilers $\mathfrak{p}$ konjugierten Fundamentalformen, welche man jetzt nach der a. S. 213 in (12a) angegebenen Bezeichnung folgendermaßen schreiben kann:

$$(5\text{a}) \qquad \begin{matrix} w_1\,, & w_2\,, & \ldots\, w_e\,, \\ w_1^{(p)}, & w_2^{(p)}, & \ldots\, w_e^{(p)}, \\ \vdots & & \\ w_1^{(p^{f-1})}, & w_2^{(p^{f-1})}, & \ldots\, w_e^{(p^{f-1})}. \end{matrix}$$

Hier ist allgemein:

$$(5\text{b}) \qquad w_i^{(p^k)} = U_0^{(p^k)} + U_1^{(p^k)} \pi_i^{(p^k)} + U_2^{(p^k)} (\pi_i^{(p^k)})^2 + \cdots,$$

und man erhält die Koeffizienten $U_\lambda^{(p^k)}$ dadurch aus den entsprechenden Linearformen U_h, daß dort alle Koffizienten durch ihre $(p^k)^{\text{ten}}$ Potenzen ersetzt werden, während entsprechend die Primzahlen $\pi_i^{(p^k)}$ die Wurzeln derjenigen Eisensteinschen Gleichung $\psi(x, \eta^{p^k}) = 0$ sind, deren linke Seite aus derjenigen von (4) durch dieselben Substitutionen hervorgeht.

Alle diese $\lambda = ef$ konjugierten Fundamentalformen genügen nun für den Bereich von $\mathfrak{p}$ einer Gleichung des λ^{ten} Grades:

$$(6) \quad F_0(w) = \prod_{i=1}^{e} \prod_{k=0}^{f-1} (w - w_i^{(p^k)}) = w^\lambda + U_1^{(0)} w^{\lambda-1} + \cdots + U_\lambda^{(0)} = 0 \qquad (\mathfrak{p}),$$

deren Koeffizienten $U_1^{(0)}, U_2^{(0)}, \ldots U_\lambda^{(0)}$ homogene Funktionen des ersten, zweiten, ... λ^{ten} Grades von $u_1, \ldots u_n$ mit rationalen p-adischen Koeffizienten sind. Legt man hier den Unbestimmten u_i alle möglichen modulo p ganzen bzw. alle gebrochenen rationalen Zahlwerte bei, so erhält man die Gleichungen, denen alle ganzen bzw. alle gebrochenen algebraischen Zahlen von $K(\alpha)$ für den Bereich von $\mathfrak{p}$ genügen. Aus diesem Grunde will ich die Gleichung (6) die Fundamentalgleichung des Körpers $K(\alpha)$ für den Bereich des Primteilers $\mathfrak{p}$ nennen. Diese Gleichung ist offenbar im Bereiche der rationalen p-adischen Zahlen unzerlegbar, d. h. sie zerfällt für unbestimmte u_i nicht in rationale p-adische Faktoren niedrigeren Grades, denn sonst würden ja auch alle Gleichungen, denen die Zahlen von $K(\alpha)$ für den Bereich von $\mathfrak{p}$ genügen, ebenfalls zerfallen, während schon die den Körper definierende Zahl α selbst für den Bereich von $\mathfrak{p}$ primitiv ist, d. h. einer irreduktiblen Gleichung des λ^{ten} Grades genügt.

Wendet man das soeben gefundene Resultat auf alle Primteiler $\mathfrak{p}_i$ von p an, so ergibt sich der Satz:

Zu jedem Primteiler $\mathfrak{p}_i$ von p vom Grade f_i und der Ordnung e_i gehört eine für den Bereich von p irreduktible Fundamentalgleichung

$$(6a) \qquad F_i(w) = 0 \qquad (i = 1, 2, \cdots h)$$

des Grades $e_i f_i = \lambda_i$ mit rationalen p-adischen Koeffizienten, der die λ_i für diesen Primteiler konjugierten Fundamentalformen für unbestimmte $u_1, u_2, \ldots u_n$ genügen.

Ist also:

$$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_h^{e_h}$$

die Zerlegung der Primzahl p in ihre Primteiler für den Körper n^{ter} Ordnung $K(\alpha)$, und $F(w) = 0$ die Fundamentalgleichung n^{ten} Grades, so ergibt die Zusammenfassung der bzw. zu $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_h$ gehörigen konjugierten Linearfaktoren die folgende Zerlegung der Funktion $F(w)$ in irreduktible Faktoren für den Bereich von p:

$$(7) \qquad F(w) = F_1(w)\, F_2(w) \cdots F_h(w) \quad (p),$$

wo allgemein $F_i(w) = 0$ die zu dem Primteiler $\mathfrak{p}_i$ gehörige Fundamentalgleichung (6a) ist.

Um nun die Potenz von p zu bestimmen, welche in der Diskriminante der Fundamentalgleichung

$$\mathfrak{D}(F) = \prod_{k > l} (w_k - w_l)^2 \qquad (k, l = 1, 2, \cdots n)$$

enthalten ist, brauche ich nur zu untersuchen, durch welche Potenz von p jede einzelne Differenz $w_k - w_l$ von je zwei konjugierten Fundamentalformen für unbestimmte $(u_1, \ldots u_n)$ genau teilbar ist. Ist nun eine bestimmte Differenz etwa $w_1 - w_2$ genau durch p^ϱ teilbar, so ist auch die entsprechende Differenz $\gamma_1 - \gamma_2$ von je zwei konjugierten ganzen Zahlen **mindestens** durch dieselbe Potenz von p teilbar, da jede ganze algebraische Zahl nebst ihren konjugierten aus den konjugierten Fundamentalformen durch eine ganzzahlige Spezialisierung $(u_i = a_i)$ der Unbestimmten hervorgeht; umgekehrt ist $w_1 - w_2$ **höchstens** durch p^σ teilbar, wenn eine ganze Zahl γ existiert, für welche $\gamma_1 - \gamma_2$ genau durch p^σ teilbar ist.

Mit Hilfe dieser einfachen Bemerkung kann nun die vorliegende Aufgabe überraschend leicht gelöst werden: Gehören zunächst die beiden konjugierten Fundamentalformen w_k und w_l zu zwei verschiedenen Primteilern von p, so ist die Differenz $w_k - w_l$ für unbestimmte $u_1, \ldots u_n$ durch p gar nicht teilbar, denn wir hatten ja a. S. 228 unten

gezeigt, daß man eine ganze p-adische Zahl γ so finden kann, daß z. B. $\gamma_k = 1$ und $\gamma_l = 0$ wird und dann ist ja $\gamma_k - \gamma_l = 1$ also durch p nicht teilbar.

Es mögen nun zweitens w_k und w_l zu demselben Primteiler $\mathfrak{p}$ von p gehören. Ist wieder e die Ordnung und f der Grad von $\mathfrak{p}$, so sollen also w_k und w_l irgend zwei unter den $\lambda = ef$ konjugierten Fundamentalformen sein, welche wir in (5a) so angeordnet hatten:

$$(8)\qquad \begin{array}{llll} w_1, & w_2, & \ldots & w_e, \\ w_1^{(p)}, & w_2^{(p)}, & \ldots & w_e^{(p)}, \\ \vdots & & & \\ w_1^{(p^{f-1})}, & w_2^{(p^{f-1})}, & \ldots & w_e^{(p^{f-1})}, \end{array}$$

Gehören nun w_k und w_l zwei verschiedenen Zeilen dieses Systemes an, so ist $w_k - w_l$ wieder für unbestimmte u_i nicht durch p teilbar. In der Tat, setzt man speziell: $w_1 = \eta$, wo η eine Zahl des Koeffizientenkörpers ist, welche zum Exponenten f selber paßt, so wird ja:

$$w_1 = w_2 = \cdots = w_e = \eta,$$

und entsprechend werden alle Zahlen der zweiten, dritten, ... f^{ten} Reihe einander gleich und zwar bzw. gleich $\eta^p, \eta^{p^2}, \ldots \eta^{p^{f-1}}$; da nun diese f Potenzen nach der über η gemachten Voraussetzung alle verschieden sind, so kann auch keine Differenz $w_k - w_l$ für unbestimmte u_h p enthalten, wenn w_k und w_l verschiedenen Reihen unseres Schemas angehören.

Es mögen jetzt endlich die konjugierten Formen w_k und w_l beide derselben etwa der ersten Horizontalreihe unseres Schemas angehören. Dann sind sie also für den zugehörigen Koeffizientenkörper $K(\eta)$ konjugiert, und ihre Entwicklungen haben die Form:

$$(9)\qquad \begin{aligned} w_k &= U_0 + U_1\pi_k + U_2\pi_k^2 + \cdots, \\ w_l &= U_0 + U_1\pi_l + U_2\pi_l^2 + \cdots, \end{aligned}$$

wo die U_i p-adische Formen des Koeffizientenkörpers $K(\eta)$ sind. Dann folgt aus der Gleichung:

$$(9\text{a})\qquad w_k - w_l = (\pi_k - \pi_l)\,(U_1 + U_2(\pi_k + \pi_l) + \cdots),$$

daß die Differenz $w_k - w_l$ für variable $u_1, \ldots u_n$ mindestens durch $\pi_k - \pi_l$ teilbar ist; sie kann aber auch keine höhere Potenz von $\mathfrak{p}$ enthalten als in $(\pi_k - \pi_l)$ enthalten ist; setzt man nämlich, was ja stets möglich ist, $w_k = \pi_k$ also $w_l = \pi_l$, so wird $w_k - w_l = \pi_k - \pi$

selbst, d. h. $w_k - w_l$ kann wirklich keine höhere Potenz von $\mathfrak{p}$ enthalten. Wir können also den folgenden wichtigen Satz aussprechen:

(10) Sind $w_1, w_2, \ldots w_n$ die n konjugierten Fundamentalformen eines Körpers n^{ter} Ordnung, und ist p eine beliebige Primzahl, so sind von den Differenzen $w_k - w_l$ alle und nur diejenigen durch eine Potenz von p mit positivem Exponenten teilbar, in welchen w_k und w_l zu demselben Primteiler $\mathfrak{p}$ von p gehören und außerdem für den zugehörigen Koeffizientenkörper $K(\eta)$ konjugiert sind. Ist das der Fall, so ist $w_k - w_l$ für unbestimmte $u_1, \ldots u_n$ genau durch diejenige Potenz von $\mathfrak{p}$ teilbar, welche in der Differenz $\pi_i - \pi_k$ der zugehörigen konjugierten Primzahlen enthalten ist.

Hieraus folgt zunächst, daß die Diskriminante der in der ersten Reihe von (8) stehenden Zahlen $w_1, w_2, \ldots w_e$ genau durch die in

$$\prod_{i,k=1}^{e}(\pi_i - \pi_k)^2 = |\pi_1^h, \pi_2^h, \cdots \pi_e^h|^2$$

enthaltene Potenz von p, also nach (10) a. S. 219 genau durch $p^{\bar{e}-1}$ teilbar ist, und wörtlich dasselbe gilt für die Diskriminanten der in der zweiten, dritten, ... f^{ten} Zeile stehenden Formen. Also ist die Diskriminante aller ef zu $\mathfrak{p}$ gehörigen Fundamentalformen in (8) genau durch

$$p^{f(\bar{e}-1)} = n(\mathfrak{p}^{\bar{e}-1})$$

teilbar. Da endlich dasselbe für jeden der h zu p gehörigen Primteiler gilt, und außerdem die Differenz $w_k - w_l$ zweier zu verschiedenen Primteilern gehörigen Fundamentalformen p gar nicht enthält, so folgt, daß die ganze Fundamentaldiskriminante genau durch

$$n(\mathfrak{p}_1^{\bar{e}_1-1} \ldots \mathfrak{p}_h^{\bar{e}_h-1})$$

teilbar ist, also p genau so oft enthält als die Körperdiskriminante. Da aber p ganz beliebig gewählt war, so ist hiermit der Fundamentalsatz bewiesen:

(11) Die Diskriminante der Fundamentalgleichung $\mathfrak{D}(u_1, \ldots u_n)$ ist eine homogene Form der Unbestimmten $u_1, u_2, \ldots u_n$, deren Zahlenteiler genau gleich der Körperdiskriminante ist.

§ 3. Die gemeinsamen außerwesentlichen Teiler der Gleichungsdiskriminanten eines Körpers.

Aus den Resultaten des vorigen Abschnittes folgt, daß die Diskriminante der Fundamentalgleichung:

$$(1)\qquad d(1, w, w^2, \cdots w^{n-1}) = |1, w_i, w_i^2, \cdots w_i^{n-1}|^2 = D \cdot |U_k^{(i)}|^2$$

gleich der Körperdiskriminante D multipliziert mit einer primitiven Form $|U_k^{(i)}|^2$ ist, daß sie also außer jener Körperdiskriminante keinen einzigen Zahlenteiler besitzt. Legt man nun in der Fundamentalform:

$$(1\text{a})\qquad w = u_1 \eta^{(1)} + u_2 \eta^{(2)} + \cdots + u_n \eta^{(n)}$$

den Unbestimmten alle möglichen ganzzahligen Werte $u_i = a_i$ bei, so erhält man alle ganzen Zahlen

$$(1\text{b})\qquad \gamma = a_1 \eta^{(1)} + a_2 \eta^{(2)} + \cdots + a_n \eta^{(n)}$$

jenes Körpers, und durch die gleichen Substitutionen ergeben sich aus (1) alle zu diesen ganzen Zahlen gehörigen Gleichungsdiskriminanten:

$$(2)\qquad d(1, \gamma, \gamma^2, \cdots \gamma^{n-1}) = |1, \gamma_i, \gamma_i^2, \cdots \gamma_i^{n-1}|^2 = D |A_k^{(i)}|^2.$$

Könnte man nun γ so auswählen, daß die ganze Zahl $|A_k^{(i)}|^2$ gleich Eins würde, so bildeten die n Potenzen $(1, \gamma, \ldots \gamma^{n-1})$ ein Fundamentalsystem für den Körper $K(\alpha)$, d. h. alle ganzen Zahlen $\bar{\gamma}$ dieses Körpers wären in der Form:

$$(3)\qquad \bar{\gamma} = b_0 + b_1 \gamma + \cdots + b_{n-1} \gamma^{n-1}$$

mit ganzzahligen Koeffizienten darstellbar; und dann würde die arithmetische Theorie dieser algebraischen Zahlen nicht die geringste Schwierigkeit bieten. In der Tat könnte man dann die zu einer beliebigen Primzahl p gehörigen Primteiler $\mathfrak{p}$, ihre Ordnung und ihren Grad, sowie auch die zu jedem dieser Teiler gehörigen Primzahlen π auf höchst einfache Weise direkt herleiten, wie im § 1 des elften Kapitels näher dargelegt werden wird.

Nun zeigte sich bald, daß es im allgemeinen nicht möglich ist, für jeden Körper $K(\alpha)$ eine dieser Forderung genügende ganze Zahl γ zu finden. Man würde aber genau dieselbe Vereinfachung der ganzen Theorie erhalten, wenn man für jede einzelne reelle Primzahl p eine ganze Zahl γ so bestimmen könnte, daß die n Potenzen $(1, \gamma, \gamma^2, \ldots \gamma^{n-1})$ nur ein Fundamentalsystem für diese Primzahl bildeten, so daß alle modulo p ganzen Zahlen in der Form (3) mit

modulo p ganzen Koeffizienten darstellbar wären. Hierzu wäre nur erforderlich, die Koeffizienten u_i in (1) durch solche ganzen Zahlen a_i zu ersetzen, daß die ganze Zahl $|A_k^{(i)}|^2$ nur nicht durch p teilbar wäre, während sie sehr wohl andere Teiler besitzen könnte; denn dann folgt ja aus (2) daß die Diskriminante $d(1, \gamma, \ldots \gamma^{n-1})$ diese Primzahl nicht öfter enthält als die Körperdiskriminante D, daß also diese n Potenzen $(1, \gamma, \ldots \gamma^{n-1})$ wirklich ein Fundamentalsystem modulo p bilden.

Ehe man die eigentümlichen Schwierigkeiten dieser Theorie genauer erkannt hatte, erschien es beinahe als selbstverständlich, daß für eine jede Primzahl p eine solche Zahl γ bestimmt werden könnte, und so hat es auch nicht an Versuchen gefehlt, auf dieser Grundlage eine allgemeine Theorie der algebraischen Zahlen aufzubauen. Aber wunderbarer Weise zeigte sich, daß es für gewisse Primzahlen p nicht möglich war, ein solches Fundamentalsystem $(1, \gamma, \ldots \gamma^{n-1})$ zu finden.

Das erste Beispiel dieser Art hatte Herr Dedekind bei dem durch die irreduktible kubische Gleichung

$$(4) \qquad F(x) = x^3 - x^2 - 2x - 8 = 0$$

definierten Körper $K(\bar{\alpha})$ gefunden. Für die Diskriminante der allgemeinen kubischen Gleichung

$$x^3 + a_1 x^2 + a_2 x + a_3 = (x - \bar{\alpha}_1)(x - \bar{\alpha}_2)(x - \bar{\alpha}_3) = 0$$

gilt die folgende Darstellung (vgl. z. B. Webers Algebra Bd. I, S. 169 (10)):

$$(5) \qquad d(1, \bar{\alpha}, \bar{\alpha}^2) = a_1^2 a_2^2 + 18 a_1 a_2 a_3 - 4 a_2^3 - 4 a_1^3 a_3 - 27 a_3^2,$$

und hieraus ergibt sich in unserem Falle:

$$(5a) \qquad d(1, \bar{\alpha}, \bar{\alpha}^2) = -2012 = -2^2 \cdot 503.$$

Hiernach ist die Körperdiskriminante entweder -503 oder $-4 \cdot 503$, weil die zur ersten Potenz erhobene Primzahl 503 nicht in dem quadratischen außerwesentlichen Teiler vorkommen kann. Wir werden nun leicht beweisen, nicht nur daß die Primzahl 2 in der Tat ein außerwesentlicher Diskriminantenteiler ist, sondern auch, daß sie als gemeinsamer außerwesentlicher Divisor in allen Gleichungsdiskriminanten dieses kubischen Körpers enthalten ist.

Hier, wie bei den anderen später gefundenen speziellen Körpern erschien aber zunächst das Auftreten dieser gemeinsamen außerwesentlichen Teiler als eine sehr seltene Anomalie, welche allerdings deshalb besonders unbequem und störend empfunden wurde, weil für sie und für sie allein die Theorie der Primteiler in völlig anderer

Weise entwickelt werden mußte. Außerdem war bei jenen ersten Betrachtungen der innere Grund, warum diese gemeinsamen außerwesentlichen Teiler auftraten, keineswegs klar.

Die vorher durchgeführten Betrachtungen zeigen nun sofort, daß das Auftreten solcher gemeinsamen außerwesentlichen Diskriminantenteiler eigentlich keine Ausnahme, sondern die Regel ist, und sie enthüllen zugleich den höchst einfachen Grund dieser scheinbar wunderbaren Tatsache. Um diese Einsicht zunächst möglichst deutlich zu geben, betrachte ich den einfachen Fall, daß die den Körper n^{ter} Ordnung $K(\alpha)$ definierende Grundgleichung für den Bereich einer Primzahl p in n rationale p-adische Linearfaktoren zerfällt, daß also für den Bereich von p die folgende Zerlegung dieser Grundgleichung besteht:

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \quad (p), \tag{6}$$

wo die Wurzeln

$$\alpha_i = a_0^{(i)} + a_1^{(i)} p + a_2^{(i)} p^2 + \cdots \quad (p) \tag{6a}$$

ganze p-adische Zahlen, ihre Koeffizienten $a^{(i)}$ also Zahlen der Reihe $0, 1, \cdots p-1$ sind. Dann zerfällt also p innerhalb $K(\alpha)$ in n voneinander verschiedene Primteiler $\mathfrak{p}_i$, deren Grad f_i und deren Ordnung e_i gleich Eins ist. Endlich ist nach dem Satze auf S. 232 die Körperdiskriminante durch p nicht teilbar.

Ist nun $\gamma = \varphi(\alpha)$ irgend eine ganze Zahl des Körpers $K(\alpha)$, so sind die n konjugierten Zahlen $\gamma_1, \gamma_2, \ldots \gamma_n$ in derselben Weise für den Bereich von p darstellbar, d. h. es bestehen n Gleichungen:

$$\begin{aligned} \gamma_1 &= b_0^{(1)} + b_1^{(1)} p + b_2^{(1)} p^2 + \cdots, \\ \gamma_2 &= b_0^{(2)} + b_1^{(2)} p + b_2^{(2)} p^2 + \cdots, \\ &\cdots\cdots\cdots\cdots \\ \gamma_n &= b_0^{(n)} + b_1^{(n)} p + b_2^{(n)} p^2 + \cdots, \end{aligned} \quad (p) \tag{6b}$$

in denen alle Koeffizienten $b^{(i)}$ ebenfalls Zahlen der Reihe $0, 1, \cdots p-1$ sind. Also gilt für die Diskriminante von γ, d. h. für das Differenzenprodukt dieser konjugierten Zahlen $(\gamma_1, \gamma_2, \ldots \gamma_n)$ die Kongruenz:

$$d(1, \gamma, \cdots \gamma^{n-1}) = \prod_{i>k} (\gamma_i - \gamma_k)^2 \equiv \prod_{i>k} (b_0^{(i)} - b_0^{(k)})^2 \pmod{p}. \tag{6c}$$

Nehmen wir nun weiter an, daß p kleiner ist als der Grad n der Grundgleichung, so ist das Differenzenprodukt der n Anfangsglieder $b_0^{(1)}, b_0^{(2)}, \ldots b_0^{(n)}$ stets durch p teilbar, wie diese Anfangsglieder auch gewählt sein mögen; in der Tat können ja diese n Zahlen $b_0^{(i)}$ nur die p Werte $0, 1, \ldots p-1$ haben, und da p kleiner als n ist, so müssen mindestens

zwei unter ihnen gleich sein. Es ergibt sich also zunächst der merkwürdige Satz:

Ist p eine Primzahl, welche kleiner ist als der Grad n des Körpers $K(\alpha)$, und welche im Bereiche dieses Körpers in n verschiedene Primteiler zerfällt, so ist p ein gemeinsamer außerwesentlicher Diskriminantenteiler dieses Körpers.

Die Primzahl p muß hier also einfach aus dem Grunde in allen Gleichungsdiskriminanten als Teiler auftreten, weil die Anzahl der modulo p inkongruenten Zahlen kleiner ist als die Anzahl der konjugierten Zahlen. Dieser Satz ist also nur eine einfache Verallgemeinerung jener bekannten trivialen Tatsachen, welche in der elementaren Zahlenlehre z. B. in den Sätzen ausgesprochen werden:

Das Differenzenprodukt

$$(u_1 - u_2)(u_2 - u_3)(u_3 - u_1)$$

von drei beliebigen ganzen Zahlen ist stets eine gerade Zahl, das Differenzenprodukt

$$(u_1 - u_2)(u_2 - u_3)(u_3 - u_4)(u_4 - u_1)(u_1 - u_3)(u_2 - u_4)$$

von vier beliebigen ganzen Zahlen ist stets ein Multiplum von sechs, usw.

Aus dem soeben bewiesenen Satze folgt bereits, daß bei der Dedekindschen Gleichung (4) die Primzahl 2 gemeinsamer außerwesentlicher Teiler aller Gleichungsdiskriminanten des zugehörigen Körpers ist. Die linke Seite dieser Gleichung zerfällt nämlich für den Bereich von 2 in drei rationale dyadische Linearfaktoren; denn da die Gleichungsdiskriminante $-2^2 \cdot 503$ für den Bereich von 2 die Ordnungszahl $\delta = 2$ besitzt, so braucht man nach dem a. S. 68 oben bewiesenen Satze nur zu zeigen, daß jene Funktion modulo $2^{\delta+1} = 8$ betrachtet drei inkongruente Linearfaktoren besitzt. Aus der Kongruenz:

$$x^3 - x^2 - 2x - 8 \equiv x(x+1)(x-2) \pmod 8$$

folgt also, daß für den Bereich von 2 eine Zerlegung besteht

$$x^3 - x^2 - 2x - 8 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \quad (2),$$

in welcher $\alpha_1, \alpha_2, \alpha_3$ ganze dyadische Zahlen sind, welche modulo 4 betrachtet bzw. kongruent $0, -1, 2$ sind. Also zerfällt 2 innerhalb $K(\alpha)$ in drei verschiedene Primfaktoren ersten Grades, und somit ist diese Primzahl nach dem soeben bewiesenen Satze wirklich ein gemeinsamer außerwesentlicher Teiler aller Gleichungsdiskriminanten dieses Körpers.

§ 4. Die notwendigen und hinreichenden Bedingungen dafür, daß eine Primzahl p gemeinsamer außerwesentlicher Diskriminantenteiler eines Körpers $K(\alpha)$ ist.

Ich wende mich nun zur vollständigen Beantwortung der Frage, unter welcher Bedingung eine gegebene Primzahl p nicht gemeinsamer außerwesentlicher Teiler der Gleichungsdiskriminanten aller ganzen Zahlen eines Körpers $K(\alpha)$ ist. Dies ist dann und nur dann der Fall, wenn man innerhalb dieses Körpers eine ganze Zahl γ so auswählen kann, daß ihre Diskriminante:

$$d(\gamma) = \prod_{i>k} (\gamma_i - \gamma_k)^2$$

diese Primzahl nicht öfter enthält als die Diskriminante

$$\mathfrak{D}(u_1 \cdots u_n) = \prod_{i>k} (w_i - w_k)^2$$

der Fundamentalgleichung, oder, was ganz dasselbe ist, wenn man γ so auswählen kann, daß jede der $\frac{n(n-1)}{2}$ Differenzen $\gamma_i - \gamma_k$ keine höhere Potenz von p als Teiler enthält, als die Differenz $w_i - w_k$ der entsprechenden konjugierten Fundamentalformen. Eine solche ganze algebraische Zahl soll für den Bereich von p regulär heißen.

Nach dem a. S. 270 oben bewiesenen Satze ist nun γ dann und nur dann für den Bereich von p regulär, wenn allein diejenigen Differenzen $\gamma_i - \gamma_k$ eine Potenz von p mit positivem Exponenten als Teiler enthalten, für welche γ_i und γ_k zu demselben Primteiler $\mathfrak{p}$ von p gehören und außerdem für den zugehörigen Koeffizientenkörper $K(\eta)$ konjugiert sind; und zwar muß dann $\gamma_i - \gamma_k$ genau durch die in der Differenz $\pi_i - \pi_k$ enthaltene Potenz von p teilbar sein. Kann man keine solche Zahl γ finden, so ist p außerwesentlicher Teiler aller Gleichungsdiskriminanten von $K(\alpha)$.

Ich untersuche zunächst, wie eine Zahl γ gewählt werden muß, damit sie sich nur in bezug auf einen Primteiler $\mathfrak{p}$ von p regulär verhalte, d. h. daß nur die Differenzen $\gamma_i - \gamma_k$ der zu $\mathfrak{p}$ gehörigen konjugierten Zahlen dieselbe Potenz von p enthalten, wie die entsprechenden Differenzen $w_i - w_k$ der konjugierten Fundamentalformen. Sind wieder e und f die Ordnung und der Grad von $\mathfrak{p}$, so bilden nach (12a) a. S. 213 die ef zu $\mathfrak{p}$ gehörigen konjugierten Zahlen das folgende Schema:

$$(1) \qquad \begin{array}{llll} \gamma_1, & \gamma_2, & \ldots & \gamma_e, \\ \gamma_1^{(p)}, & \gamma_2^{(p)}, & \ldots & \gamma_e^{(p)}, \\ \vdots & & & \\ \gamma_1^{(p^{f-1})}, & \gamma_2^{(p^{f-1})}, & \ldots & \gamma_e^{(p^{f-1})}, \end{array}$$

von denen immer die in derselben Horizontalreihe stehenden für den Bereich des zugehörigen Koeffizientenkörpers $K(\eta)$ konjugiert sind. Dann lassen sich die e konjugierten Zahlen γ_i der ersten Reihe nach (5) a. S. 209 folgendermaßen nach Potenzen einer Primzahl π_i entwickeln:

(2) $$\gamma_i = \eta_0 + \eta_1 \pi_i + \eta_2 \pi_i^2 + \cdots \qquad (i = 1, 2, \cdots e),$$

wo $\eta_0, \eta_1, \eta_2, \ldots$ bestimmte $(p^f-1)^{\text{te}}$ Wurzeln der Einheit oder Null bedeuten, also im ganzen p^f verschiedene Werte haben können; und man kann nach dem a. S. 228 unten bewiesenen Satze die p-adische Zahl γ stets so wählen, daß jene Entwicklungskoeffizienten η_k beliebig gegebene Werte aus der Reihe jener p^f möglichen erhalten. Allgemein haben dann die entsprechenden Zahlen der $(h+1)^{\text{ten}}$ Horizontalreihe in (1) die folgenden Entwicklungen:

(2a) $$\gamma_i^{(p^h)} = \eta_0^{p^h} + \eta_1^{p^h} \pi_i^{(p^h)} + \eta_2^{p^h} (\pi_i^{(p^h)})^2 + \cdots \qquad \binom{i = 1, 2, \cdots e}{h = 0, 1, \cdots f-1}.$$

Soll nun γ zunächst für den Bereich von $\mathfrak{p}$ regulär sein, so müssen die f Anfangsglieder

(2b) $$\eta_0,\ \eta_0^p,\ \eta_0^{p^2},\ \ldots\ \eta_0^{p^{f-1}}$$

der in der ersten, zweiten, ... f^{ten} Zeile von (1) stehenden konjugierten Zahlen voneinander verschieden sein; denn wäre z. B. $\eta_0^{p^2} = \eta_0$, so wäre ja jede Differenz $\gamma_i^{(p^2)} - \gamma_k$ von je einer Zahl der ersten und der dritten Zeile mindestens durch $\mathfrak{p}$ teilbar, γ wäre also sicher nicht regulär für den Bereich von $\mathfrak{p}$. Nach der a. S. 191 (6c) gemachten Bemerkung sind jene f Anfangsglieder (2b) dann und nur dann alle verschieden, wenn das erste Anfangsglied η_0, also auch jedes andere $\eta_0^{p^h}$, zum Exponenten f selbst, und nicht zu einem eigentlichen Teiler von f paßt. Soll aber zweitens jede Differenz

$$\gamma_i - \gamma_k = (\pi_i - \pi_k)\,(\eta_1 + \eta_2(\pi_i - \pi_k) + \cdots)$$

von irgend zwei der ersten Zeile angehörigen Zahlen genau durch die in $\pi_i - \pi_k$ enthaltene Potenz von p teilbar sein, so muß nur $\eta_1 \gtrless 0$ sein; ist dies der Fall, so sind von selber auch die entsprechenden Koeffizienten $\eta_1^{p^h}$ von Null verschieden, d. h. auch die Differenzen $\gamma_i^{(p^h)} - \gamma_k^{(p^h)}$ von irgend zwei Zahlen der $(h+1)^{\text{ten}}$ Reihe sind auch nur durch die in $\pi_i^{(p^h)} - \pi_k^{(p^h)}$ enthaltene Potenz von p genau teilbar. Es ergibt sich also zunächst der Satz:

> Eine Zahl γ ist dann und nur dann in bezug auf einen Primteiler f^{ten} Grades $\mathfrak{p}$ regulär, wenn die Anfangsglieder ihrer zu $\mathfrak{p}$ gehörigen Entwicklungen (2) zum Exponenten f selber passen, während die Koeffizienten von π nur von Null verschieden zu sein brauchen.

Nach der oben gemachten Bemerkung kann beiden Forderungen zugleich stets genügt werden, und zwar kann γ so gewählt werden, daß η_0 irgend eine zum Exponenten f passende und η_1 eine beliebige Einheitswurzel etwa gleich Eins ist.

Es ist jetzt nur noch zu untersuchen, wie die p-adische Zahl γ gewählt werden muß, damit sie in bezug auf die Primzahl p selbst regulär sei. Ist wieder:

(3) $$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_h^{e_h}$$

die Zerlegung von p in seine Primfaktoren, so muß γ zunächst in bezug auf jeden dieser h Primteiler regulär sein; ist also allgemein f_i der Grad von $\mathfrak{p}_i$, so müssen die Anfangsglieder der zu $\mathfrak{p}_i$ gehörigen konjugierten Zahlen zum Exponenten f_i selber passen, und die nächsten Koeffizienten von Null verschieden sein. Ferner aber, und das ist die einzige noch weiter hinzutretende Bedingung, müssen die Entwicklungen:

$$\gamma' = \eta_0' + \eta_1'\pi' + \eta_2'\pi'^2 + \cdots,$$
$$\gamma'' = \eta_0'' + \eta_1''\pi'' + \eta_2''\pi_2''^2 + \cdots$$

von irgend zwei zu verschiedenen Primteilern $\mathfrak{p}'$ und $\mathfrak{p}''$ gehörigen konjugierten Zahlen so beschaffen sein, daß ihre Differenz durch keine Potenz von p mit positivem Exponenten teilbar ist.*) Da nun für die kleinste in π' und π'' zugleich enthaltene Potenz p^ϱ von p offenbar die Kongruenz:

$$\gamma' - \gamma'' \equiv \eta_0' - \eta_0'' \pmod{p^\varrho},$$

besteht, so ist jene Differenz nur dann durch p^ϱ teilbar, wenn:

$$\eta_0' \equiv \eta_0'' \quad (\text{mod.}\, p^\varrho)$$

ist, und zwar müssen hier η_0' und η_0'' bzw. $(p^{f'}-1)^{\text{te}}$ und $(p^{f''}-1)^{\text{te}}$ Wurzeln der Einheit sein, welche zu den Exponenten f' und f'' passen.

---

*) Hier, wie in der ganzen folgenden Untersuchung, sollen die den Primteilern $\mathfrak{p}$ entsprechenden Primzahlen π so gewählt sein, daß sie durch den zugehörigen Divisor $\mathfrak{p}$ nur einmal, aber durch jeden der $(h-1)$ konjugierten Teiler $\mathfrak{p}'$ mindestens so oft teilbar sind, wie die Primzahl p selbst. Nach dem a. S. 228 unten bewiesenen Satze kann man stets p-adische Zahlen finden, welche dieser Forderung genügen, und aus dem a. S. 282 abgeleiteten allgemeinen Theoreme folgt weiter, daß derselben Forderung auch immer durch gewöhnliche algebraische Zahlen genügt werden kann. Ist die Entwicklungszahl π so gewählt, so ist sie durch die gebrochene Potenz $p^{\frac{1}{e}}$, aber durch keine höhere Potenz von p algebraisch teilbar, denn sie enthält ja $\mathfrak{p}$ genau so oft als $p^{\frac{1}{e}}$, jeden anderen Primteiler $\mathfrak{p}'$ aber mindestens so oft als p selbst. Zwei zu $\mathfrak{p}'$ und $\mathfrak{p}''$ gehörige Primzahlen π' und π'' sind beide durch p^ϱ teilbar, wenn ϱ der kleinere unter den Brüchen $\frac{1}{e'}$ und $\frac{1}{e''}$ ist.

Eine solche Kongruenz kann aber nur dann bestehen, wenn $\eta_0' = \eta_0''$ mithin $f' = f''$ ist, wenn also die Primteiler $\mathfrak{p}'$ und $\mathfrak{p}''$ von gleichem Grade sind. In der Tat genügen ja η_0' und η_0'' für den Bereich von p irreduktiblen Gleichungen des f'^{ten} und f''^{ten} Grades, deren nullte Näherungswerte auch modulo p betrachtet irreduktibel bleiben, und diese können somit modulo p^ϱ nur dann eine Wurzel gemeinsam haben, wenn jene irreduktiblen Funktionen modulo p kongruent sind, wenn also $f'' = f'$ ist. Da endlich alle voneinander verschiedenen $(p^{f'} - 1)^{\text{ten}}$ Einheitswurzeln nach S. 190 (3) und (3a) auch modulo p inkongruent sind, so muß in der Tat $\eta_0' = \eta_0''$ sein.

Ordnet man also die h Primteiler von p nach ihrem Grade f, und sind allgemein die λ_f Primfaktoren:

$$\overset{(f)}{\mathfrak{p}}_1, \overset{(f)}{\mathfrak{p}}_2, \ldots \overset{(f)}{\mathfrak{p}}_{\lambda_f} \qquad (f = 1, 2, \cdots) \tag{4}$$

alle diejenigen, welche denselben Grad f besitzen, so tritt zu den vorher ausgesprochenen Bedingungen dafür, daß γ für den Bereich von p regulär sei, noch die folgende weitere hinzu:

Die Anfangsglieder der zu den λ_f Primteilern f^{ten} Grades gehörigen konjugierten Zahlen müssen alle voneinander verschieden sein.

Ist nun γ irgend eine ganze algebraische Zahl des Körpers $K(\alpha)$, und sind allgemein die Anfangsglieder der zu dem Divisor $\overset{(f)}{\mathfrak{p}}_i$ gehörigen konjugierten Zahlen

$$\overset{(i)}{\eta}_0, \overset{(i)}{\eta}{}_0^{p}, \overset{(i)}{\eta}{}_0^{p^2}, \ldots \overset{(i)}{\eta}{}_0^{p^{f-1}}, \qquad (i = 1, 2, \cdots \lambda_f),$$

so müssen alle diese $f\lambda_f$ $(p^f - 1)^{\text{ten}}$ Einheitswurzeln zum Exponenten f selbst passen und voneinander verschieden sein, wenn γ regulär sein soll. Nun gibt es aber nur eine endliche Anzahl von $(p^f - 1)^{\text{ten}}$ Einheitswurzeln, welche zum Exponenten f passen. Ich will deren Anzahl durch $g(f)$ bezeichnen; sie wird im § 6 mit den einfachsten Hilfsmitteln bestimmt werden. Dann ergibt sich aus den soeben durchgeführten Betrachtungen sehr einfach der folgende Satz, durch den die Frage nach den gemeinsamen außerwesentlichen Teilern eines Körpers $K(\alpha)$ vollständig und höchst einfach gelöst wird:

Es sei:

$$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_h^{e_h}$$

die Zerlegung einer Primzahl p innerhalb des Körpers $K(\alpha)$, und es geben die Zahlen $\lambda_1, \lambda_2, \ldots \lambda_f, \ldots$ an, wie viele unter diesen h verschiedenen Primteilern vom Grade $1, 2, \ldots f, \ldots$ sind. Ist dann allgemein $g(f)$ die Anzahl der $(p^f - 1)^{\text{ten}}$ Einheitswurzeln, welche zum Exponenten f passen, so ist p dann

und nur dann gemeinsamer außerwesentlicher Teiler aller Gleichungsdiskriminanten von $K(\alpha)$, wenn von den Ungleichungen:

$$(5)\qquad \begin{aligned} \lambda_1 &> g(1),\\ 2\lambda_2 &> g(2),\\ &\vdots\\ f\lambda_f &> g(f)\\ &\vdots \end{aligned}$$

wenigstens eine erfüllt ist; denn allein in diesem Falle ist es unmöglich, in dem Körper $K(\alpha)$ eine für den Bereich von p reguläre Zahl γ aufzufinden.

Zum Beweise dieses merkwürdigen Satzes nehme ich erstens an, es sei für alle Grade f

$$f\lambda_f \leqq g(f) \qquad (f=1,2,\cdots$$

und zeige zunächst, daß man unter den ganzen p-adischen Zahlen von $K(\alpha)$ stets eine in bezug auf p reguläre Zahl γ finden kann. Es seien nämlich allgemein für $f=1,2,\ldots$

$$(6)\qquad \overset{(i)}{\eta}_0,\ \overset{(i)}{\eta}{}_0^p,\ \ldots\ \overset{(i)}{\eta}{}_0^{p^{f-1}} \qquad (i=1,2,\cdots\lambda_f)$$

$f\lambda_f$ voneinander verschiedene zum Exponenten f passende $(p^f-1)^{\text{te}}$ Einheitswurzeln, welche ja, da n. d. V. $f\lambda_f \leqq g(f)$ ist, stets gefunden werden können. Wählt man dann, was wieder stets möglich ist, die p-adische algebraische Zahl γ so aus, daß die zu dem i^{ten} Primteiler f^{ten} Grades $\overset{(i)}{\mathfrak{p}}_f$ gehörigen Wurzeln die Anfangsglieder (6) haben, während das folgende Glied erster Ordnung einen beliebigen von Null verschiedenen Koeffizienten, etwa den Koeffizienten 1 besitzt, so ist ja allen vorher aufgestellten Bedingungen genügt, γ ist also wirklich eine für den Bereich von p reguläre Zahl.

Ist dagegen auch nur eine jener Bedingungen (5) nicht erfüllt, ist also z. B. für ein bestimmtes f:

$$f\lambda_f > g(f),$$

so müssen unter den $f\lambda_f$ Anfangsgliedern derjenigen zu einer beliebigen Zahl konjugierten Wurzeln, welche zu den λ_f Primteilern f^{ten} Grades $\overset{(f)}{\mathfrak{p}}_i$ gehören, sicher gleiche vorkommen, weil es eben nicht $f\lambda_f$ verschiedene zum Exponenten f passende $(p^f-1)^{\text{te}}$ Einheitswurzeln gibt; es ist also in diesem Falle wirklich nicht möglich, eine für den Bereich von p reguläre Zahl γ zu finden.

In dem a. S. 273 durchgeführten Beispiele besaß p innerhalb des Körpers n^{ter} Ordnung n Primfaktoren ersten Grades; hier ist also

$$\lambda_1 = n, \quad \lambda_2 = \lambda_3 = \cdots = 0,$$

während die Anzahl $g(1)$ aller verschiedenen p-adischen Zahlen, welche zum Exponenten Eins passen, welche also der Gleichung

$$x^p - x = 0 \quad (p)$$

genügen, gleich p ist. Aus unserem allgemeinen Satze folgt also genau wie vorher, daß p dann und nur dann gemeinsamer außerwesentlicher Diskriminantenteiler von $K(\alpha)$ ist, wenn

$$1 \cdot \lambda_1 > g(1) \quad \text{d. h.} \quad \text{wenn} \quad n > p$$

ist.

§ 5. Die Beziehungen zwischen den gewöhnlichen und den p-adischen algebraischen Zahlen eines Körpers.

Durch die soeben durchgeführten Betrachtungen ist zunächst nur der Beweis geführt, daß allein unter den oben angeführten Bedingungen (5) a. S. 279 eine für den Bereich von p reguläre p-adische Zahl in dem Körper $K(\alpha)$ gefunden werden kann. Es könnte aber sehr wohl möglich sein, daß auch in diesem Falle keine gewöhnliche algebraische Zahl existiert, welche den an eine reguläre Zahl zu stellenden Forderungen genügt. Dieses Bedenken wird nun durch den folgenden allgemeinen Satz leicht beseitigt werden:

> Ist β eine beliebig gegebene p-adische Zahl des Körpers $K(\alpha)$, so kann man in demselben Körper stets eine gewöhnliche algebraische Zahl finden, welche jener für eine beliebig hohe Potenz p^{k+1} als Modul kongruent ist.

In der Tat, sei

$$(1) \qquad \gamma^{(1)}, \gamma^{(2)}, \ldots \gamma^{(n)}$$

ein beliebiges Fundamentalsystem für die ganzen Zahlen von $K(\alpha)$, dessen Elemente $\gamma^{(i)}$ also gewöhnliche (nicht p-adische) algebraische Zahlen sind; dann ist die gegebene p-adische Zahl β durch dieses System in der Form:

$$(2) \qquad \beta = u_1\gamma^{(1)} + u_2\gamma^{(2)} + \cdots + u_n\gamma^{(n)}$$

darstellbar, wo die Koeffizienten u_i rationale p-adische Zahlen sind. Sind dann $u_1^{(k)}, u_2^{(k)}, \ldots u_n^{(k)}$ die k^{ten} Näherungswerte jener Koeffizienten, so besitzt die gewöhnliche (nicht p-adische) algebraische Zahl desselben Körpers:

$$(2\text{a}) \qquad \beta^{(k)} = u_1^{(k)}\gamma^{(1)} + u_2^{(k)}\gamma^{(2)} + \cdots + u_n^{(k)}\gamma^{(n)},$$

welche der k^{te} Näherungswert von β in bezug auf das System $(\gamma^{(1)}, \dots \gamma^{(n)})$ genannt werden soll, offenbar die Eigenschaft, daß

$$\beta \equiv \beta^{(k)} \pmod{p^{k+1}}$$

ist, weil ja in der Differenz $\beta - \beta^{(k)}$ alle Glieder $(u_h - u_h^{(k)})\gamma^{(h)}$ mindestens durch p^{k+1} teilbar sind, und zwar ist für alle n konjugierten Zahlen:

$$\beta_i \equiv \beta_i^{(k)} \pmod{p^{k+1}};$$

damit ist unser Satz bewiesen.

Ich benutze diesen allgemeinen Satz zunächst zu dem Nachweise, daß, falls innerhalb $K(\alpha)$ eine für p reguläre p-adische Zahl β existiert, sicher auch eine reguläre gewöhnliche Zahl in demselben Bereiche gefunden werden kann. Zu diesem Zwecke drücke ich wie in (2) die p-adische Zahl β durch das obige Fundamentalsystem (1) aus, und bilde den ersten Näherungswert von β in bezug auf das System, d. h. die gewöhnliche algebraische Zahl:

$$\beta^{(1)} = u_1^{(1)}\gamma^{(1)} + u_2^{(1)}\gamma^{(2)} + \cdots + u_n^{(1)}\gamma^{(n)},$$

deren Koeffizienten $u_h^{(1)}$ die ersten Näherungswerte der Zahlen u_h sind. Dann besteht für alle n zu β konjugierten Zahlen die Kongruenz:

$$\beta_i \equiv \beta_i^{(1)} \pmod{p^2}.$$

Also ist a fortiori für jeden Primteiler $\mathfrak{p}_i$ von p:

$$\beta_i \equiv \beta_i^{(1)} \pmod{\mathfrak{p}_i^2},$$

d. h. die Entwicklungen der konjugierten Zahlen β_i und $\beta_i^{(1)}$ stimmen alle mindestens in den beiden Anfangsgliedern überein. Da sich aber die Bedingungen dafür, daß β regulär ist, allein auf die beiden Anfangsglieder der Zahlen β_i beziehen, so ist $\beta^{(1)}$ wirklich dann und nur dann für den Bereich von p regulär, wenn es β ist, und damit ist unsere letzte Behauptung, also auch das Theorem a. S. 279 vollständig bewiesen.

Ich benutze dieses Resultat noch weiter, um auf die merkwürdige prinzipiell wichtige Beziehung hinzuweisen, welche zwischen den p-adischen und den gewöhnlichen algebraischen Zahlen des Körpers $K(\alpha)$ besteht. Im zweiten Kapitel war gezeigt worden, daß eine rationale p-adische Zahl jede Reihe

$$A = a_r p^r + a_{r+1} p^{r+1} + a_{r+2} p^{r+2} + \cdots$$

ist, deren Koeffizienten a_i völlig beliebige modulo p reduzierte ganze Zahlen sein können. Eine solche Zahl ist für den Bereich von p im

allgemeinen nicht einer gewöhnlichen rationalen Zahl gleich, aber es können stets rationale Zahlen, nämlich ihre Näherungswerte genügend hoher Ordnung, gefunden werden, welche diesen Zahlen für den Bereich von p mit jeder vorgegebenen Genauigkeit gleich sind.

Genau ebenso zeigt sich jetzt, daß die konjugierten p-adischen algebraischen Zahlen eines Körpers $K(\alpha)$ für den Bereich dieser Primzahl als Reihen

$$\gamma_i = \overset{(i)}{\eta}_r \pi_i^r + \overset{(i)}{\eta}_{r+1} \pi_i^{r+1} + \cdots \qquad (i = 1, 2, \ldots n)$$

dargestellt werden können, deren Koeffizienten innerhalb des zugehörigen Koeffizientenkörpers $K(\overset{(i)}{\eta})$ in der Weise beliebig angenommen werden können, daß die zu den verschiedenen Primfaktoren

$$\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_k$$

von p gehörigen konjugierten Entwicklungen völlig unabhängig voneinander sind (vgl. S. 228 unten).

Diese konjugierten p-adischen Zahlen

$$\gamma_1, \gamma_2, \ldots \gamma_n$$

sind dann für den Bereich von p im allgemeinen nicht gewöhnlichen konjugierten Zahlen desselben Körpers gleich, wohl aber folgt aus den soeben durchgeführten Betrachtungen, daß es gewöhnliche konjugierte Zahlen desselben Körpers gibt, nämlich ihre Näherungswerte

$$\gamma_1^{(k)}, \gamma_2^{(k)}, \ldots \gamma_n^{(k)}$$

von genügend hoher Ordnung k, welche diesen Zahlen für den Bereich von p mit jeder vorgegebenen Genauigkeit gleich sind. Hieraus folgt sofort der wichtige Satz:

> Man kann stets eine gewöhnliche algebraische Zahl des Körpers $K(\alpha)$ finden, deren n Konjugierte bestimmt vorgegebene Entwicklungskoeffizienten bis zu den Gliedern einer beliebig hohen Ordnung besitzen.

In der Tat kann man ja eine p-adische Zahl γ finden, für welche die den einzelnen Primteilern $\mathfrak{p}_k$ entsprechenden Entwicklungen völlig beliebig vorgeschrieben werden können, und ihre Näherungswerte $\gamma^{(k)}$ sind dann gewöhnliche algebraische Zahlen, deren Entwicklungen mit denen von γ für alle n konjugierten bis zu den durch p^{k+1} teilbaren Gliedern übereinstimmen.

Ist also z. B. $\mathfrak{p}$ ein Primteiler von p vom Grade f und von der Ordnung e, so gibt es in dem Körper $K(\alpha)$ im allgemeinen keine gewöhnliche algebraische Zahl, deren zu $\mathfrak{p}$ gehörige Entwicklungen bzw.

gleich $\eta, \eta^p, \ldots \eta^{p^f-1}$ sind, wo η eine primitive $(p^f-1)^{te}$ Einheitswurzel bedeutet, während die zu jedem anderen Primteiler $\mathfrak{p}'$ gehörigen konjugierten Zahlen alle gleich Null sind. Wohl aber gibt es gewöhnliche Zahlen, deren konjugierte jenen Einheitswurzeln für eine beliebig hohe Potenz p^{k+1} kongruent bzw. durch eine beliebig hohe Potenz von p algebraisch teilbar sind. Ebenso gibt es im allgemeinen keine gewöhnliche algebraische Zahl π, deren ef für den Bereich von $\mathfrak{p}$ konjugierte bzw. gleich

$$\sqrt[e]{\eta p}, \quad \sqrt[e]{\eta^p p}, \ldots \sqrt[e]{\eta^{p^f-1} p}$$

sind, wo die e^{te} Wurzel in ihren e verschiedenen Bedeutungen angenommen wird, während alle übrigen konjugierten Zahlen gleich Null sind, wohl aber kann man in diesem Körper gewöhnliche algebraische Zahlen finden, deren konjugierte jenen Zahlen für jede noch so hohe Potenz von p als Modul kongruent sind.

Eine wie große Genauigkeit für den Bereich von p also auch gefordert werde, immer kann man in dem Körper $K(\alpha)$ gewöhnliche algebraische Zahlen finden, durch welche die in die Rechnung eingeführten p-adischen Zahlen unbedenklich ersetzt werden können, genau ebenso, wie eine jede irrationale Zahl mit jeder vorgegebenen Genauigkeit ihrer Größe nach durch ihre rationalen Näherungswerte ersetzt werden kann.

Auf S. 317 (4) wird im Anschluß an diese Betrachtungen der Nachweis geführt werden, daß man stets algebraische Zahlen des Körpers $K(\alpha)$ finden kann, welche für den Bereich von beliebig vielen auch zu verschiedenen reellen Primzahlen gehörigen Primteilern $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots \mathfrak{s}$ beliebig vorgegebene Entwicklungen bis zu Gliedern beliebig hoher Ordnung haben, und welche sich sonst überall regulär verhalten.

Auch in der Theorie der algebraischen Funktionen einer Variabeln gelingt es, wie hier beiläufig erwähnt werde, die n Wurzeln $u_1, u_2 \ldots u_n$ einer algebraischen Gleichung n^{ten} Grades:

$$f(u, z) = 0$$

für u mit rationalen Funktionen von z als Koeffizienten in der Umgebung einer Stelle $z = a$ in Potenzreihen zu entwickeln, von denen immer je e nach ganzen Potenzen von $(z-a)^{\frac{1}{e}}$ fortschreiten und konjugiert sind, wenn diese zu einem und demselben e-blättrigen Verzweigungspunkte gehören; und dieselben Entwicklungen gelten für jede rationale Funktion $w = \varphi(u, z)$ von z und u, d. h. für jede Funktion des zugehörigen Körpers $K(z, u)$.

Betrachtet man allgemeiner die Gesamtheit aller rationalen Funktionen $\overline{w} = \overline{\varphi}(u, z)$ von u deren Koeffizienten jetzt nur in der Um-

gebung der Stelle $(z = a)$ konvergente Potenzreihen von rationalem Charakter sind, so lassen diese in der Umgebung jener Stelle genau dieselben Entwicklungen zu, wie die Funktionen des Körpers $K(z, u)$, mit der Maßgabe, daß man stets eine Funktion $\bar{w}$ finden kann, welche in der Umgebung der zur Stelle $z = a$ gehörigen Verzweigungspunkte beliebig vorgegebene Entwicklungen $\bar{w}_1, \ldots \bar{w}_n$ besitzt. Eine solche Funktion $\bar{w}$ wird im allgemeinen nicht dem Körper $K(z, u)$ angehören, also nicht rational von u und von z abhängen, jedoch man zeigt auch hier, daß man innerhalb dieses Körpers Funktionen w finden kann, welche in der Umgebung der Stelle $(z = a)$ mit jeder vorgegebenen Genauigkeit mit $\bar{w}$ übereinstimmen d. h. beliebig vorgegebene Entwicklungen besitzen. So kann man z. B. stets Funktionen jenes Körpers finden, deren konjugierte in der Umgebung eines e-blättrigen Verzweigungspunktes mit beliebiger Annäherung gleich $(z - a)^{\frac{1}{e}}$ selbst sind, während sie in der Umgebung jeder anderen zu $(z = a)$ gehörigen Stelle mit der gleichen Annäherung gleich Null werden.

§ 6. Die Anzahl $g(f)$ der zum Exponenten f passenden $(p^f - 1)^{\text{ten}}$ Einheitswurzeln.

Zur vollständigen Lösung der Frage nach den gemeinsamen außerwesentlichen Diskriminantenteilern eines Körpers $K(\alpha)$ fehlt noch die Bestimmung der Anzahl $g(f)$ aller zum Exponenten f passenden $(p^f - 1)^{\text{ten}}$ Einheitswurzeln. Ich löse diese Frage einfach dadurch, daß ich die Gleichung

$$(1) \qquad G_{f_0}(x) = \prod (x - \overset{(f_0)}{\eta}) = 0$$

aufsuche, deren einfache Wurzeln alle und nur die zum Exponenten f_0 passenden Einheitswurzeln $\overset{(f_0)}{\eta}$ sind, wenn f_0 irgend einen Teiler von f oder f selbst bedeutet. Dann ist der Grad dieser Gleichung die gesuchte Anzahl $g(f_0)$.

Nach den a. S. 189 flgde. hergeleiteten Sätzen kann nun jene Funktion $G_{f_0}(x)$ sehr leicht bestimmt werden. Da nämlich die Gleichung des $(p^f)^{\text{ten}}$ Grades

$$H_f(x) = x^{p^f} - x = \prod (x - \eta) = 0$$

alle und nur die Einheitswurzeln η als einfache Wurzeln enthält, welche zu f oder zu einem Teiler von f passen, so findet man, wenn man rechts immer alle zu einem und demselben Exponenten f_0 passenden

Linearfaktoren $(x - \overset{(f_0)}{\eta})$ zusammenfaßt und ihr Produkt durch $G_{f_0}(x)$ bezeichnet, die Gleichung

$$H_f(x) = x^{p^f} - x = \prod_{f_0 | f} G_{f_0}(x), \tag{2}$$

wo die Multiplikation rechts über alle Teiler f_0 von f auszudehnen ist; und diese Gleichung besteht identisch für jedes beliebige f. Wählt man z. B. $f = 6$ und schreibt außerdem noch die entsprechenden Gleichungen für alle Teiler 3, 2 und 1 von 6 hin, so erhält man nun die vier Gleichungen:

$$\begin{aligned} H_6(x) &= G_6(x)\, G_3(x)\, G_2(x)\, G_1(x), \\ H_3(x) &= \qquad\;\; G_3(x) \qquad\;\; G_1(x), \\ H_2(x) &= \qquad\qquad\qquad G_2(x)\, G_1(x), \\ H_1(x) &= \qquad\qquad\qquad\qquad\;\; G_1(x), \end{aligned} \tag{2a}$$

und aus ihnen berechnen sich die vier Funktionen $G(x)$ auf der rechten Seite leicht folgendermaßen:

$$\begin{aligned} G_6(x) &= \frac{H_6(x)\, H_1(x)}{H_3(x)\, H_2(x)} = \frac{(x^{p^6} - x)\,(x^p - x)}{(x^{p^3} - x)\,(x^{p^2} - x)}, \\ G_3(x) &= \frac{H_3(x)}{H_1(x)} = \frac{x^{p^3} - x}{x^p - x}, \\ G_2(x) &= \frac{H_2(x)}{H_1(x)} = \frac{x^{p^2} - x}{x^p - x}, \\ G_1(x) &= H_1(x) = x^p - x. \end{aligned} \tag{3a}$$

Also ergeben sich für die gesuchten Anzahlen $g(6)$, $g(3)$, $g(2)$, $g(1)$ die Werte:

$$\begin{aligned} g(6) &= p^6 - p^3 - p^2 + p, \qquad & g(3) &= p^3 - p, \\ g(2) &= p^2 - p, & g(1) &= p. \end{aligned} \tag{2c}$$

Genau ebenso kann nun allgemein die zu einem beliebigen Exponenten f gehörige Funktion $G_f(x)$ bestimmt werden. Schreibt man nämlich auch hier die Gleichung (2) für f und alle Teiler f_0 von f hin, so erhält man wieder genau so viele Gleichungen

$$H_{f_0}(x) = \prod_{\bar{f}_0 | f} G_{\bar{f}_0}(x), \tag{3}$$

als f Teiler f_0 besitzt, in denen rechts jedesmal über alle Teiler $\bar{f}_0$ von f_0 zu multiplizieren ist. Ist also A die Anzahl aller Teiler von f, so erhält man in (3) ein System von A Gleichungen mit den A Unbekannten $G_{\bar{f}_0}(x)$, welches sehr leicht aufgelöst werden kann, und zwar ergibt eine einfache Betrachtung, daß sich die Funktion $G_f(x)$ in der

folgenden bemerkenswert einfachen Art durch die gegebenen Funktionen $H_{f_0}(x) = x^{p^{f_0}} - x$ ausdrücken läßt:

$$(4)\quad G_f(x) = \frac{H_f(x) \cdot \prod\limits_{(q,q')} H_{\frac{f}{qq'}}(x) \cdots}{\prod\limits_{(q)} H_{\frac{f}{q}}(x) \cdot \prod\limits_{(q,q',q'')} H_{\frac{f}{qq'q''}}(x) \cdots} = \frac{(x^{p^f} - x) \cdot \prod\limits_{(q,q')} (x^{p^{\frac{f}{qq'}}} - x) \cdots}{\prod\limits_{(q)} (x^{p^{\frac{f}{q}}} - x) \cdot \prod\limits_{(q,q',q'')} (x^{p^{\frac{f}{qq'q''}}} - x) \cdots}.$$

Hier bedeuten $q, q', q'', \ldots$ die sämtlichen voneinander verschiedenen Primfaktoren von f; d. h. im Zähler ist über alle und nur die Funktionen $H_{f_0}(x) = x^{p^{f_0}} - x$ zu multiplizieren, deren Exponent f_0 gleich f ist, oder eine gerade Anzahl verschiedener Primfaktoren $q, q', q'', \ldots$ weniger enthält als f, während der Nenner das Produkt aller derjenigen Funktionen $x^{p^{f_0}} - x$ ist, deren Exponent eine ungerade Anzahl verschiedener Primfaktoren weniger als f besitzt. Diejenigen Funktionen $x^{p^{f_0}} - x$, in welchen der Teiler f_0 von f auch nur zwei gleiche Primfaktoren weniger als f hat, kommen weder im Zähler noch im Nenner vor.

Zum Beweise bemerke ich zunächst, daß im Zähler und Nenner des Quotienten (4) überhaupt nur solche Linearfaktoren $x - \eta$ vorkommen, in denen η eine zum Exponenten f oder zu einem Teiler von f passende Einheitswurzel ist, da ja die im Zähler und Nenner stehenden Funktionen $H(x)$ keine anderen Linearfaktoren enthalten. Zweitens erkennt man sofort, daß jeder Linearfaktor $(x - \overset{(f)}{\eta})$ von $G_f(x)$, in welchem $\overset{(f)}{\eta}$ zum Exponenten f selber paßt, seiner Definition nach nur in $H_f(x)$ und zwar nur einmal enthalten ist, also auch auf der rechten Seite von (4) wirklich nur einmal vorkommt. Es bleibt also nur noch zu zeigen, daß jeder Linearfaktor $(x - \overset{(f_0)}{\eta})$, in welchem $\overset{(f_0)}{\eta}$ zu einem bestimmten eigentlichen Teiler f_0 von f paßt, ebenso oft im Zähler wie im Nenner von (4) vorkommt, so daß er sich aus jenem Quotienten weghebt.

Um diesen letzten Beweis zu führen, nehme ich an, es seien

$$(5)\qquad q_1, q_2, \ldots q_h$$

diejenigen voneinander verschiedenen Primzahlen, welche der eigentliche Teiler f_0 weniger oft als f enthält. Dann ist $(x - \overset{(f_0)}{\eta})$ in allen und

nur den Funktionen $H_{\frac{f}{qq'\ldots}}(x)$ enthalten, deren Index ein Multiplum von f_0 ist, und dies ist nur dann der Fall, wenn der Nenner des Index $\frac{f}{qq'\ldots}$ nur aus den Primzahlen (5) besteht. Enthält nämlich jener Nenner $qq'q''\ldots$ auch nur eine nicht in (5) vorkommende Primzahl q_0, so ist der Index $\frac{f}{qq'\ldots}$ durch f_0 nicht teilbar, weil ja f_0 die Primzahl q_0 ebenso oft enthält als f, während q_0 in dem Index einmal weniger oft auftritt. Besteht dagegen der Nenner des Index $\frac{f}{qq'\ldots}$ nur aus den Primzahlen (5), so ist der Index sicher ein Multiplum von f_0, da ja f_0 jeden dieser Primfaktoren mindestens einmal weniger enthält als f, während in dem Index nur gewisse unter ihnen einmal weniger oft vorkommen.

Also ist $(x - \overset{(f_0)}{\eta})$ in allen und nur den Funktionen $H(x)$ im Zähler und Nenner von (4) enthalten, deren Indizes die folgenden sind:

$$(6) \qquad f, \quad \frac{f}{q_i}, \quad \frac{f}{q_i q_k}, \quad \frac{f}{q_i q_k q_l}, \ldots,$$

wo $q_i, q_i q_k, q_i q_k q_l, \ldots$ die h Primzahlen (5), ihre $\frac{h(h-1)}{1 \cdot 2}$ Produkte zu je zweien, ihre $\frac{h(h-1)(h-2)}{1 \cdot 2 \cdot 3}$ Produkte zu je dreien usw. bedeuten; und zwar stehen diese Funktionen im Zähler oder im Nenner des Quotienten (4), jenachdem die Anzahl der im Nenner ihres Index stehenden Primzahlen gerade oder ungerade ist. Demnach ist der Exponent von $(x - \overset{(f_0)}{\eta})$ in jenem Quotienten gleich:

$$1 - h + \frac{h(h-1)}{1 \cdot 2} - \frac{h(h-1)(h-2)}{1 \cdot 2 \cdot 3} + \cdots \pm 1 = (1-1)^h = 0,$$

falls $h > 0$, d. h. wenn f_0 wirklich ein eigentlicher Teiler von f ist. Damit ist die Richtigkeit der Gleichung (4) vollständig bewiesen.

Aus (1) ergab sich zunächst, daß $G_f(x)$ eine ganze Funktion von α mit ganzzahligen p-adischen Koeffizienten des Körpers $K(\eta)$ ist; da aber diese Funktion nach (4) gleich dem Quotienten zweier ganzen Funktionen mit rationalen ganzzahligen Koeffizienten ist, in welchen der Koeffizient der höchsten Potenz gleich Eins ist, so folgt, daß die Funktionen $G_f(x)$ sämtlich gewöhnliche ganzzahlige Koeffizienten besitzen.

Wir können die Darstellung (4) von $G_f(x)$ wesentlich einfacher schreiben, wenn wir in diese Gleichung die s. g. Möbiusschen Koeffizienten in der Kroneckerschen Bezeichnung einführen. Ist nämlich d eine beliebige positive ganze Zahl, so wollen wir unter dem Symbole ε_d immer die Zahl Null verstehen, wenn der Index d auch nur eine Primzahl mehr als einmal enthält. Besitzt dagegen

$$d = q_1 q_2 \cdots q_h$$

lauter verschiedene Primfaktoren, so soll $\varepsilon_d = (-1)^h$, d. h. gleich $+1$ oder gleich -1 sein, jenachdem die Anzahl dieser Primfaktoren gerade oder ungerade ist.

Dann kann man die Darstellung (4) von $G_f(x)$ offenbar in der folgenden einfachen Form schreiben:

$$(7) \qquad G_f(x) = \prod_{d \mid f} H_{\frac{f}{d}}(x)^{\varepsilon_d} = \prod_{d d' = f} H_{d'}(x)^{\varepsilon_d},$$

wo das erste Produkt auf der rechten Seite über alle Teiler d von f, das zweite über alle Zerlegungen von $f = dd'$ in zwei komplementäre Faktoren zu erstrecken ist; denn wegen der Eigenschaften der Möbiusschen Koeffizienten werden ja alle Potenzen $H_{\frac{f}{d}}(x)^{\varepsilon_d}$ gleich Eins, in denen der Nenner d auch nur eine Primzahl mehrfach enthält, da ihr Exponent $\varepsilon_d = 0$ ist.

Aus der Gleichung (4) oder (7) ergibt sich endlich die Anzahl der zum Exponenten f passenden Einheitswurzeln $\overset{(f)}{\eta}$ gleich dem Grade von $G_f(x)$; es ist also:

$$(8) \qquad g(f) = p^f - \sum_{(q)} p^{\frac{f}{q}} + \sum_{(q,q')} p^{\frac{f}{qq'}} - \sum_{(q,q',q'')} p^{\frac{f}{qq'q''}} + \cdots$$
$$= \sum_{d \mid f} \varepsilon_d \, p^{\frac{f}{d}} = \sum_{d d' = f} \varepsilon_d \, p^{d'}.$$

Diese Zahl muß ein Vielfaches von f sein, denn die zum Exponenten f passenden Einheitswurzeln lassen sich ja in Reihen

$$(9) \qquad \eta_i, \; \eta_i^p, \; \eta_i^{p^2}, \; \ldots \; \eta_i^{p^{f-1}}$$

zu je f Gliedern anordnen, welche alle untereinander verschieden sind.

Auf Grund der soeben gewonnenen Erkenntnis können wir jetzt das Resultat der im § 4 durchgeführten Untersuchung folgendermaßen aussprechen:

> Ist allgemein λ_f die Anzahl der verschiedenen Primfaktoren vom Grade f, welche die Primzahl p in dem Körper $K(\alpha)$ besitzt, so ist p dann und nur dann gemeinsamer außerwesentlicher Diskriminantenteiler des Körpers $K(\alpha)$, wenn von den Ungleichungen:
>
> $$\lambda_f > \frac{1}{f}\Big(\sum_{d d' = f} \varepsilon_d p^{d'}\Big) \qquad (f = 1, 2, \cdots)$$
>
> mindestens eine erfüllt ist.

§ 7. Anderes Kriterium für die gemeinsamen außerwesentlichen Diskriminantenteiler. Die Ergänzungskörper für einen Körper in bezug auf eine Primzahl.

Aus der soeben durchgeführten Untersuchung geht hervor, daß in der Diskriminante der Fundamentalgleichung

$$(1) \qquad \mathfrak{D}(u_1, \cdots u_n) = \mathfrak{D} \cdot \mathfrak{E}(u_1, \cdots u_n)$$

für einen Körper $K(\alpha)$ die primitive Form $\mathfrak{E}(u_1, u_2, \ldots u_n)$, obwohl sie als Funktion der Unbestimmten u_i keinen Zahlenteiler besitzt, doch für alle ganzzahligen Wertsysteme dieser Unbestimmten einen und denselben Primteiler p als Faktor enthalten kann. In diesem Falle ist p gemeinsamer außerwesentlicher Teiler aller Gleichungsdiskriminanten von $K(\alpha)$. Man kann nun, wie noch kurz bewiesen werden soll, dieselbe Frage auch ganz ohne Kenntnis der Natur der primitiven Form $\mathfrak{E}(u_1, \ldots u_n)$ mit Hilfe des folgenden leicht zu beweisenden Hilfssatzes lösen:

> Eine ganze ganzzahlige Form $\mathfrak{E}(u_1, \ldots u_n)$ ist dann und nur dann für alle ganzzahligen u_i durch eine Primzahl p teilbar, wenn sie das Modulsystem
>
> $$(2) \qquad P = (p, u_1^p - u_1, u_2^p - u_2, \cdots u_n^p - u_n)$$
>
> enthält, d. h. wenn sie folgendermaßen darstellbar ist:
>
> $$(2a) \quad \mathfrak{E}(u_i) = p\,\mathfrak{G}_0(u_i) + (u_1^p - u_1)\,\mathfrak{G}_1(u_i) + \cdots + (u_n^p - u_n)\,\mathfrak{G}_n(u_i),$$
>
> wo die Koeffizienten $\mathfrak{G}_k(u_i)$ ebenfalls ganze ganzzahlige Funktionen der Unbestimmten $u_1, \ldots u_n$ sind.

Zunächst ist jede das Modulsystem P enthaltende, also in der Form (2a) darstellbare Funktion $\mathfrak{E}(u_1, \ldots u_n)$ für alle ganzzahligen Werte der Unbestimmten u_i durch p teilbar, weil die n Differenzen $(u_k^p - u_k)$ nach dem Fermatschen Satze für jeden ganzzahligen Wert $u_i = a_i$ diese Primzahl enthalten. Um nun auch umgekehrt zu zeigen, daß dieselbe Bedingung (2a) notwendig ist, beachte ich, daß jede ganze ganzzahlige Funktion $\mathfrak{E}(u_i)$ offenbar in der folgenden Form geschrieben werden kann:

$$(3) \qquad \mathfrak{E}(u_i) = \mathfrak{E}_0(u_i) + p\,\mathfrak{G}_0(u_i) + \sum_{k=1}^{n} (u_k^p - u_k)\,\mathfrak{G}_k(u_i),$$

wo die „reduzierte Funktion“ $\mathfrak{E}_0(u_i)$ in bezug auf jede der n Unbestimmten von niedrigerem als dem p^{ten} Grade ist, und alle ihre Koeffizienten Zahlen der Reihe $0, 1, \ldots p-1$ sind; und nach der soeben gemachten Bemerkung besteht dann für jedes ganzzahlige Wertsystem $(u_i = a_i)$ die Kongruenz:

$$\mathfrak{E}(a_i) \equiv \mathfrak{E}_0(a_i) \pmod{p}.$$

Es braucht somit nur noch bewiesen zu werden, daß eine solche reduzierte Funktion $\mathfrak{E}_0(u_1, \dots u_n)$ nur dann für alle ganzzahligen Werte $(u_i = a_i)$ durch p teilbar ist, wenn sie Null ist.

Entwickelt man nun $\mathfrak{E}_0(u_i)$ nach Potenzen einer ihrer Unbestimmten, etwa von u_n, so ergibt sich:

$$\mathfrak{E}_0(u_i) = \overline{\mathfrak{E}}_0(u_1, \cdots u_{n-1}) + \overline{\mathfrak{E}}_1(u_1, \cdots u_{n-1})\, u_n + \cdots$$
$$+ \overline{\mathfrak{E}}_{p-1}(u_1, \cdots u_{n-1})\, u_n^{p-1},$$

wo nun die Koeffizienten $\overline{\mathfrak{E}}_k(u_1, \dots u_{n-1})$ genau ebensolche „reduzierte" Funktionen sind, wie $\mathfrak{E}_0(u_1, \dots u_n)$, welche aber nur $(n-1)$ Unbestimmte enthalten. Legt man jetzt den Größen $u_1, \dots u_{n-1}$ irgend ein ganzzahliges Wertsystem $a_1, \dots a_{n-1}$ bei, so muß die Funktion des $(p-1)^{\text{ten}}$ Grades der einen Unbestimmten u_n:

$$\mathfrak{E}_0(a_1, \cdots a_{n-1}, u_n) = \overline{\mathfrak{E}}_0(a_l) + \overline{\mathfrak{E}}_1(a_l)\, u_n + \cdots + \overline{\mathfrak{E}}_{p-1}(a_l)\, u_n^{p-1}$$
$$(l = 1, 2, \cdots n-1)$$

für die p inkongruenten Werte

$$u_n = 0, 1, \cdots p-1$$

durch p teilbar sein, und dies ist nur möglich, wenn die p Koeffizienten $\overline{\mathfrak{E}}_k(a_l)$ sämtlich durch p teilbar sind; da nun dasselbe gelten muß, wie auch das ganzzahlige Wertsystem $(a_1, \dots a_{n-1})$ gewählt ist, so folgt, daß die reduzierte Form $\mathfrak{E}_0(u_1, \dots u_n)$ dann und nur dann für alle ganzzahligen Werte ihrer n Unbestimmten durch p teilbar ist, wenn dasselbe für die p reduzierten Funktionen $\overline{\mathfrak{E}}_k(u_1, \dots u_{n-1})$ von den $(n-1)$ Unbestimmten $u_1, \dots u_{n-1}$ der Fall ist, welche die Koeffizienten der einzelnen Potenzen $1, u_n, \dots u_n^{p-1}$ bilden. Schließt man in derselben Weise weiter fort, so ergibt sich zuletzt, daß $\mathfrak{E}_0(u_1, \dots u_n)$ nur dann die verlangte Eigenschaft besitzt, wenn alle ihre einzelnen Zahlkoeffizienten p enthalten, oder, da diese modulo p reduziert angenommen werden konnten, wenn sie alle Null sind; und damit ist unsere Behauptung vollständig bewiesen.

Wenden wir diesen Satz auf die Körperdiskriminante an, so ergibt sich sofort das folgende Resultat:

(4) Eine Primzahl p ist dann und nur dann gemeinsamer außerwesentlicher Teiler aller Gleichungsdiskriminanten von $K(\alpha)$, wenn der primitive Bestandteil der Körperdiskriminante das Modulsystem $P = (p;\, u_i^p - u_i)$ enthält.

Die Reduktion der primitiven Form $\mathfrak{E}(u_1, \dots u_n)$ für das Modulsystem P wird durch die Bemerkung sehr einfach, daß für ein variables u stets die Kongruenz besteht:

(5) $$u^a \equiv u^{s_a} \pmod{(u^p - u)},$$

wenn s_a die Ziffersumme des im p-adischen Zahlensysteme dargestellten Exponenten:

(5a) $$a = a_0 + a_1 p + \cdots + a_\nu p^\nu$$

ist; in der Tat ist ja:

$$u^a = u^{a_0} \cdot (u^p)^{a_1} (u^{p^2})^{a_2} \cdots \equiv u^{a_0 + a_1 + \cdots + a_\nu} \equiv u^{s_a} \pmod{(u^p - u)}.$$

Ersetzt man also in der primitiven Form $\mathfrak{E}(u_1, \ldots u_n)$ alle Exponenten der u_i durch ihre p-adischen Ziffersummen, verkleinert diese neuen Exponenten in derselben Weise solange, bis alle Exponenten kleiner als p geworden sind und reduziert endlich alle Koeffizienten der so sich ergebenden Form modulo p auf ihre kleinsten Reste, so ist p dann und nur dann gemeinsamer außerwesentlicher Diskriminantenteiler von $K(\alpha)$, wenn jener Rest Null ist.

Da nach (5a) a. S. 264:

$$\mathfrak{E}(u_1, \ldots u_n) = |U_m^{(i)}|^2$$

das Quadrat einer homogenen Form der $\left(\frac{n(n-1)}{2}\right)^{\text{ten}}$ Dimension in $u_1, \ldots u_n$ ist, so gilt der weitere Satz:

Eine Primzahl kann nur dann außerwesentlicher Diskriminantenteiler für den Körper n^{ter} Ordnung $K(\alpha)$ sein, wenn sie nicht größer als $\frac{n(n-1)}{2}$ ist.

Ist nämlich $p > \frac{n(n-1)}{2}$, so sind die Exponenten der Unbestimmten u_i in $|U_m^{(i)}|$ schon für das Divisorensystem $(u_i^p - u_i)$ reduziert; also müßten alle Koeffizienten jener primitiven Form durch p teilbar sein, wenn sie für alle ganzzahligen Werte der u_i durch p teilbar sein sollte, was nicht der Fall sein kann.

Man kann den Hilfssatz (2), ohne seinen Beweis im geringsten zu ändern, in einer wesentlich allgemeineren Form aussprechen: Bei seinem Beweise wurden nämlich nur die beiden Voraussetzungen gebraucht, daß die n Kongruenzen:

$$u_i^p - u_i \equiv 0 \pmod{p} \qquad (i = 1, 2, \cdots n)$$

im Körper $K(1)$ der rationalen Zahlen genau so viele inkongruente Wurzeln haben als ihr Grad angibt, und daß p innerhalb dieses Körpers eine Primzahl ist. Wählt man daher zunächst anstelle jener n Funktionen $u_i^p - u_i$ irgendwelche ganzzahlige Funktionen

$$F_1(u_1), \cdots F_n(u_n)$$

bzw. von $u_1, u_2, \cdots u_n$ so, daß jede der n Kongruenzen

$$F_i(u_i) \equiv 0 \pmod{p}$$

genau so viele inkongruente Wurzeln besitzt als ihr Grad angibt, so folgt wörtlich ebenso wie vorher der allgemeinere Satz:

(6) Eine ganze ganzzahlige Funktion $\mathfrak{G}(u_1, \cdots u_n)$ ist dann und nur dann für alle Wurzeln der n ganzzahligen Kongruenzen:

$$F_1(u_1) \equiv 0, \quad F_2(u_2) \equiv 0, \cdots F_n(u_n) \equiv 0 \pmod p$$

deren jede genau so viele hat, als ihr Grad beträgt, durch p teilbar, wenn sie das Modulsystem

$$\bar{P} = (p, F_1(u_1)), \cdots F_n(u_n))$$

enthält.

Eine weitere Verallgemeinerung dieses Hilfssatzes erhalte ich, wenn ich anstelle des Körpers $K(1)$ der rationalen Zahlen einen beliebigen algebraischen Körper $K(\beta)$ zu Grunde lege; nur muß dann statt der reellen Primzahl natürlich ein Primteiler $\mathfrak{p}$ einer reellen Primzahl p innerhalb $K(\beta)$ als Modul gewählt werden. Besitzen dann die n Funktionen $F_i(u_i)$ innerhalb $K(\beta)$ soviele inkongruente Wurzeln modulo $\mathfrak{p}$, als ihr Grad angibt, so ist eine Funktion $\mathfrak{G}(u_1, \cdots u_n)$ dann und nur dann für alle Wurzeln der n Kongruenzen

(7) $$F_i(u_i) \equiv 0 \pmod{\mathfrak{p}}$$

durch $\mathfrak{p}$ teilbar, wenn sie das Modulsystem:

(8) $$(\mathfrak{p}, F_1(u_1), \ldots F_n(u_n))$$

enthält.

Endlich mache ich noch die besondere Voraussetzung, daß sowohl die zu untersuchende Funktion $\mathfrak{G}(u_1, \ldots u_n)$, als auch jene n Funktionen $F_i(u_i)$ nicht algebraische Koeffizienten des Körpers $K(\beta)$, sondern ganze Zahlen von $K(1)$ besitzen, daß die letzteren aber innerhalb des Körpers $K(\beta)$ so viele modulo $\mathfrak{p}$ inkongruente Wurzeln haben, als ihr Grad angibt. Auch dann gilt natürlich der zuletzt bewiesene Satz; reduziert man aber die Funktion $\mathfrak{G}(u_1, \ldots u_n)$ zunächst für das Modulsystem $(F_1(u_1), \ldots F_n(u_n))$ auf seinen kleinsten Rest, so erhält man eine ganzzahlige Funktion des Körpers $K(1)$, deren sämtliche Koeffizienten dann und nur dann durch den Primteiler $\mathfrak{p}$ teilbar sind, wenn sie die zugehörige Primzahl p selbst enthalten.

Unter dieser Voraussetzung ist demnach die ganze Funktion $\mathfrak{G}(u_1, \ldots u_n)$ dann und nur dann für alle algebraischen Wurzeln der Kongruenzen

(9) $$F_i(u_i) \equiv 0 \pmod{\mathfrak{p}}$$

durch den algebraischen Primteiler $\mathfrak{p}$ teilbar, wenn sie das rationale Modulsystem:

$$(p, F_1(u_1), \ldots F_n(u_n))$$

enthält.

Diesen Satz benutze ich, um eine interessante Erweiterung des Problemes der außerwesentlichen Diskriminantenteiler zu geben. Man kann nämlich etwa auftretende gemeinsame Diskriminantenteiler eines Körpers $K(\alpha)$ dadurch beseitigen, daß man die Koeffizienten $u_1, u_2, \ldots u_n$ der n konjugierten Fundamentalformen:

$$w_i = u_1 \xi_i^{(1)} + u_2 \xi_i^{(2)} + \cdots + u_n \xi_i^{(n)} \qquad (i = 1, 2, \cdots n)$$

nicht mehr innerhalb des Bereiches der reellen ganzen Zahlen, sondern in dem größeren Raume der ganzen algebraischen Zahlen eines anderen Körpers beliebig annimmt. Es sei nämlich wieder $\mathfrak{E}(u_1, \ldots u_n)$ die von ihrem Zahlenteiler, der Körperdiskriminante, befreite Diskriminante der Fundamentalgleichung. Ist dann $K(\beta)$ ein beliebiger anderer Körper, und $\mathfrak{p}$ ein Primdivisor der reellen Primzahl p für denselben, so werde zunächst untersucht, unter welcher Bedingung $\mathfrak{p}$ gemeinsamer außerwesentlicher Teiler aller Diskriminanten $\prod (w_i - w_k)$ ist, wenn man jetzt für $u_1, \ldots u_n$ nicht mehr reelle ganze Zahlen, sondern beliebige ganze algebraische Zahlen des Körpers $K(\beta)$ setzt; oder, was dasselbe ist, unter welcher Bedingung die primitive Form $\mathfrak{E}(u_1, \ldots u_n)$ stets durch $\mathfrak{p}$ teilbar ist, wenn man für $u_1, \ldots u_n$ beliebige ganze Zahlen des Bereiches $K(\beta)$ setzt.

Ist nun $\mathfrak{f}$ der Grad des Primteilers $\mathfrak{p}$ für den Körper $K(\beta)$, ist also die Anzahl der modulo $\mathfrak{p}$ inkongruenten ganzen Zahlen dieses Körpers gleich $p^{\mathfrak{f}}$, so genügt jede Zahl dieses Bereiches der Kongruenz:

$$u^{p^{\mathfrak{f}}} - u \equiv 0 \pmod{\mathfrak{p}};$$

diese Kongruenz besitzt also innerhalb $K(\beta)$ genau so viele inkongruente Wurzeln, als ihr Grad angibt. Die obige Frage kann also auch so gestellt werden: Unter welcher Bedingung ist die primitive Form $\mathfrak{E}(u_1, \ldots u_n)$ für alle Kongruenzwurzeln modulo $\mathfrak{p}$ der n Funktionen

$$u_1^{p^{\mathfrak{f}}} - u_1, \quad u_2^{p^{\mathfrak{f}}} - u_2, \quad \cdots \quad u_n^{p^{\mathfrak{f}}} - u_n$$

durch $\mathfrak{p}$ teilbar? Diese Frage wird nun unmittelbar durch den zuletzt abgeleiteten Satz beantwortet, wenn man dort die n Funktionen $F_i(u_i)$ durch $u_i^{p^{\mathfrak{f}}} - u_i$ ersetzt. Man erhält also den Satz:

(10) Der Primteiler $\mathfrak{p}$ des Körpers $K(\beta)$ ist dann und nur dann in dem soeben angegebenen Sinne gemeinsamer außerwesentlicher Teiler aller Gleichungsdiskriminanten von $K(\alpha)$, wenn die von ihrem Zahlenteiler befreite Körperdiskriminante $\mathfrak{E}(u_1, u_2, \ldots u_n)$ das Divisorensystem

$$P_{\mathfrak{f}} = \left(p;\ u_1^{p^{\mathfrak{f}}} - u_1, \cdots u_n^{p^{\mathfrak{f}}} - u_n\right)$$

enthält; hier bedeutet $\mathfrak{f}$ den Grad von $\mathfrak{p}$ für den Körper $K(\beta)$.

Da das hier gefundene Kriterium allein von dem Grade $\mathfrak{f}$ von $\mathfrak{p}$ abhängt, so gilt dasselbe für alle Divisoren von p innerhalb $K(\beta)$, welche denselben Grad besitzen.

Das hier gefundene Resultat kann nun benutzt werden, um zu entscheiden, unter welchen Bedingungen es möglich ist, die Koeffizienten $u_1, \ldots u_n$ der n konjugierten Fundamentalformen

$$w_i = u_1 \xi_i^{(1)} + u_2 \xi_i^{(2)} + \cdots + u_n \xi_i^{(n)} \qquad (i = 1, 2, \cdots n)$$

innerhalb eines Körpers $K(\beta)$ so anzunehmen, daß ihre Diskriminante

$$\mathfrak{D}(w) = \prod_{i>k} (w_i - w_k)^2 = \mathfrak{D} \cdot \mathfrak{E}(u_1, \cdots u_n)$$

keinen einzigen Primfaktor von p öfter enthält als die Körperdiskriminante, oder, was dasselbe ist, ob es möglich ist, die Unbestimmten $u_1, u_2, \ldots u_n$ innerhalb $K(\beta)$ so zu wählen, daß die primitive Form $\mathfrak{E}(u_1, \ldots u_n)$ zu p teilerfremd ist.

Offenbar muß man hierzu zunächst $u_1, \ldots u_n$ so annehmen können, daß $\mathfrak{E}(u_1, \ldots u_n)$ zu jedem einzelnen Primteiler von p relativ prim wird, d. h. es darf keiner von jenen Primdivisoren gemeinsamer außerwesentlicher Diskriminantenteiler von $K(\alpha)$ sein. Ist also:

$$p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_l^{e_l}$$

die Zerlegung von p innerhalb $K(\beta)$ und sind

$$\mathfrak{f}_1, \mathfrak{f}_2, \cdots \mathfrak{f}_l$$

die Grade der einzelnen Primteiler, so kann p nur dann die geforderte Eigenschaft haben, wenn die primitive Form kein einziges der l Divisorensysteme:

$$P_{\mathfrak{f}_i} = \left(p; u_1^{p^{\mathfrak{f}_i}} - u_1, \cdots u_n^{p^{\mathfrak{f}_i}} - u_n\right) \qquad (i = 1, 2, \cdots l)$$

enthält, wobei natürlich nur diejenigen Systeme untersucht zu werden brauchen, für welche die Zahlen $\mathfrak{f}_i$ voneinander verschieden sind.

Sind diese Bedingungen aber erfüllt, so ergibt sich leicht, daß für die Unbestimmten $u_1, \ldots u_n$ stets solche Zahlen $\beta_1, \ldots \beta_n$ des Körpers $K(\beta)$ gewählt werden können, daß die algebraische Zahl $\mathfrak{E}(\beta_1, \beta_2, \ldots \beta_n)$ zu p teilerfremd ist. Ist nämlich allgemein $\mathfrak{p}_i$ nicht gemeinsamer außerwesentlicher Diskriminantenteiler von $K(\alpha)$, so kann man n Zahlen $\beta_1^{(i)}, \ldots \beta_n^{(i)}$ so bestimmen, daß

$$\mathfrak{E}\left(\beta_1^{(i)}, \beta_2^{(i)}, \cdots \beta_n^{(i)}\right) \gtrless 0 \pmod{\mathfrak{p}_i}$$

ist. Denkt man sich nun für jeden der l Primteiler $\mathfrak{p}_i$ von p n solche Zahlen $\beta_k^{(i)}$ bestimmt, und wählt man dann, was nach dem a. S. 282 bewiesenen Satze stets möglich ist, n ganze algebraische Zahlen $\beta_1, \beta_2, \ldots \beta_n$ des Körpers $K(\beta)$, so aus, daß

$$\beta_1 \equiv \beta_1^{(i)}, \quad \beta_2 \equiv \beta_2^{(i)}, \cdots \beta_n \equiv \beta_n^{(i)} \pmod{\mathfrak{p}_i} \qquad (i = 1, 2, \cdots l)$$

wird, so ist allgemein:

$$\mathfrak{E}(\beta_1, \cdots \beta_n) \equiv \mathfrak{E}(\beta_1^{(i)}, \cdots \beta_n^{(i)}) \gtrless 0 \pmod{\mathfrak{p}_i} \qquad (i = 1, 2, \cdots l)$$

d. h. $\mathfrak{E}(\beta_k)$ ist in der Tat zu p teilerfremd.

Ich will $K(\beta)$ einen **Ergänzungskörper** zu $K(\alpha)$ in bezug auf die Primzahl p nennen, wenn man die Unbestimmten u_i der Fundamentalform von $K(\alpha)$ innerhalb $K(\beta)$ so auswählen kann, daß die Diskriminante $\prod(w_i - w_k)^2$ keinen Primteiler von p öfter enthält als die Körperdiskriminante von $K(\alpha)$. Dann kann man die notwendige und hinreichende Bedingung dafür, daß $K(\beta)$ für $K(\alpha)$ in bezug auf p ein Ergänzungskörper ist, folgendermaßen aussprechen:

(11) Es sei $p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_l^{e_l}$ die Zerlegung der reellen Primzahl p in ihre Primfaktoren innerhalb $K(\beta)$, und $\mathfrak{f}_1, \mathfrak{f}_2, \ldots \mathfrak{f}_\lambda$ seien diejenigen Grade derselben, welche voneinander verschieden sind. Dann ist $K(\beta)$ dann und nur dann ein Ergänzungskörper von $K(\alpha)$ in bezug auf p, wenn die von ihrem Zahlenfaktor befreite Diskriminante der Fundamentalgleichung von $K(\alpha)$ kein einziges der λ Divisorensysteme:

$$P_{\mathfrak{f}_1}, P_{\mathfrak{f}_2}, \ldots P_{\mathfrak{f}_\lambda}$$

enthält.

Es soll jetzt angegeben werden, welches der Ergänzungskörper niedrigsten Grades $K(\beta)$ für einen Körper $K(\alpha)$ in bezug auf eine beliebige Primzahl p ist. Zu diesem Zwecke untersuche ich die von ihrem Zahlenfaktor befreite Diskriminante der Fundamentalgleichung $\mathfrak{E}(u_1, u_2, \ldots u_n)$ auf ihre Teilbarkeit durch die Divisorensysteme:

(12) $$P_1, P_2, P_3, \ldots,$$

wo wieder allgemein:

$$P_k = (p;\ u_1^{p^k} - u_1, \cdots u_n^{p^k} - u_n)$$

ist. Enthält diese primitive Form das erste System:

$$P_1 = (p;\ u_1^p - u_1, \ldots u_n^p - u_n)$$

nicht, so ist p überhaupt nicht außerwesentlicher Teiler von $K(\alpha)$, d. h. der Ergänzungskörper niedrigster Ordnung ist der Körper $K(1)$ der rationalen Zahlen. Ist dagegen $\mathfrak{E}(u_1, \ldots, u_n)$ durch P_1 teilbar, so muß man in der Reihe $P_1, P_2, \ldots$ zuletzt zu einem Divisorensysteme $P_{\mathfrak{f}}$ kommen, welches nicht mehr in der primitiven Form $\mathfrak{E}(u_i) = |U_i^{(k)}|^2$ enthalten ist; wählt man nämlich μ so groß, daß die Potenz p^μ größer ist als die Dimension $\frac{n(n-1)}{2}$ der homogenen Form $|U_i^{(k)}|$, so wird

diese durch das Modulsystem $(u_1^{p^\mu} - u_1, \cdots u_n^{p^\mu} - u_n)$ überhaupt nicht mehr auf eine Form niedrigeren Grades reduziert, weil alle Exponenten der Unbestimmten u_i kleiner sind als p^μ. Daher könnte die Form $|U_i^{(k)}|$ also auch $\mathfrak{G}(u_i)$ nur dann das Modulsystem

$$P_\mu = (p;\, u_1^{p^\mu} - u_1, \cdots u_n^{p^\mu} - u_n)$$

enthalten, wenn alle ihre Koeffizienten durch p teilbar wären, und dies steht mit der Tatsache im Widerspruch, daß $\mathfrak{G}(u_1, \ldots u_n)$ primitiv ist. Diese Form kann somit nur eine endliche Anzahl von Divisorensystemen $P_1, P_2, \ldots$ enthalten, und zwar ist diese Anzahl sicher kleiner als μ, wenn μ die niedrigste Potenz von p bedeutet, welche größer ist als $\frac{n(n-1)}{2}$.

Es sei nun $P_\mathfrak{f}$ das erste Modulsystem der Reihe (12), welches in $\mathfrak{G}(u_i)$ nicht enthalten ist. Ist dann:

$$g(y) = y^\mathfrak{f} + b_1 y^{\mathfrak{f}-1} + \cdots + b_\mathfrak{f} = 0$$

irgend eine Gleichung des $\mathfrak{f}^{\text{ten}}$ Grades, deren linke Seite auch modulo p irreduktibel ist, und β eine ihrer $\mathfrak{f}$ Wurzeln, so zeigt man leicht, daß der durch sie konstituierte Körper $\mathfrak{f}^{\text{ter}}$ Ordnung ein Ergänzungskörper niedrigsten Grades zu $K(\alpha)$ in bezug auf p ist.

Zunächst kann man nämlich stets eine modulo p irreduktible Funktion $g(y)$ von einem beliebig vorgegebenen Grade $\mathfrak{f}$ finden, da durch jede zum Exponenten $(p^\mathfrak{f} - 1)$ gehörige $(p^\mathfrak{f} - 1)^{\text{te}}$ Einheitswurzel eine solche bestimmt wird. Ferner erkennt man sofort, daß $K(\beta)$ überhaupt ein Ergänzungskörper zu $K(\alpha)$ in bezug auf p ist. Da nämlich $g(y)$ modulo p irreduktibel ist, so ist p innerhalb $K(\beta)$ selbst eine Primzahl und ihr Grad ist gleich $\mathfrak{f}$. Die Primzahl p wäre also für den Körper $K(\beta)$ dann und nur dann gemeinsamer außerwesentlicher Teiler aller Gleichungsdiskriminanten von $K(\alpha)$, wenn $\mathfrak{G}(u_1, \ldots u_n)$ das Divisorensystem $P_\mathfrak{f} = (p;\, u_k^{p^\mathfrak{f}} - u_k)$ enthielte, was der vorher gemachten Annahme widerstreitet.

Ist endlich $K(\gamma)$ ein anderer Körper, dessen Grad kleiner ist als $\mathfrak{f}$, und ist für diesen $\bar{\mathfrak{p}}$ irgend ein Primteiler von p, so ist sein Grad $\bar{\mathfrak{f}}$ höchstens gleich dem Grade von $K(\gamma)$, also kleiner als $\mathfrak{f}$. Daher ist $\bar{\mathfrak{p}}$ sicher gemeinsamer außerwesentlicher Diskriminantenteiler von $K(\alpha)$ für den Bereich $K(\gamma)$, da die Form $\mathfrak{G}(u_i)$ das Divisorensystem $(p;\, u_i^{p^{\bar{\mathfrak{f}}}} - u_i)$ enthält, dessen Index $\bar{\mathfrak{f}}$ kleiner ist als $\mathfrak{f}$. Man erhält also den Satz:

> Ist $P_\mathfrak{f} = (p;\, u_i^{p^\mathfrak{f}} - u_i)$ das Divisorensystem niedrigster Ordnung, welches in der primitiven Form $\mathfrak{G}(u_i)$ nicht enthalten ist, so ist der niedrigste Ergänzungskörper $K(\beta)$ zu $K(\alpha)$ für

(13) die Primzahl p vom Grade $\mathfrak{f}$ und ein solcher wird durch jede ganzzahlige Gleichung $\mathfrak{f}^{\text{ten}}$ Grades konstituiert, deren linke Seite modulo p irreduktibel ist.

Für den durch die Gleichung

$$\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$$

definierten Körper $K(\alpha)$ war die Primzahl 2 gemeinsamer außerwesentlicher Diskriminantenteiler.

Da hier die Diskriminante der Fundamentalgleichung

$$\mathfrak{D}(w) = (w_1 - w_2)^2 (w_2 - w_3)^2 (w_3 - w_1)^2 = -503 \cdot \mathfrak{E}(u_1, u_2, u_3)$$

abgesehen von ihrem Zahlenteiler das Quadrat einer homogenen Funktion der dritten Dimension ist, so lehrt unser Satz, daß man das Auftreten des gemeinsamen außerwesentlichen Teilers 2 vermeiden kann, wenn man u_1, u_2, u_3 als ganze Zahlen eines Körpers $K(\beta)$ wählt welcher durch eine auch modulo 2 irreduktible quadratische Gleichung definiert ist. Wählt man speziell die Gleichung:

$$\beta^2 + \beta + 1 = \frac{\beta^3 - 1}{\beta - 1} = 0,$$

so folgt, daß in diesem Falle β als dritte Wurzel der Einheit angenommen werden kann; hier ist also der einfachste Ergänzungskörper ein Kreisteilungskörper. Es gilt auch allgemein der interessante Satz, daß für jeden Körper $K(\alpha)$ in bezug auf eine beliebige Primzahl p als Ergänzungskörper immer ein Körper von größter algebraischer Einfachheit gefunden werden kann, nämlich ein solcher, welcher durch Einheitswurzeln vom Primzahlgrade gebildet wird. Jedoch soll hierauf an dieser Stelle nicht mehr eingegangen werden. (Vgl. meine Abhandlung „Arithmetische Untersuchungen über die gemeinsamen außerwesentlichen Diskriminantenteiler einer Gattung. Crelles Journal Bd. 113, S. 128—160.)

Elftes Kapitel.

Die Darstellung der algebraischen Divisoren.

§ 1. Die Zerlegung der reellen Primzahlen in ihre Primdivisoren.

Ich will nun zeigen, wie einfach sich die Zerlegung der reellen Primzahlen in ihre Primfaktoren innerhalb des Körpers $K(\alpha)$ zunächst unter der Voraussetzung gestaltet, daß in jenem Körper eine für den Bereich von p reguläre Zahl gefunden werden kann. Für alle diejenigen Primzahlen, welche in der Diskriminante $d(\alpha)$ der Grundgleichung gar nicht enthalten sind, ist die Zahl α selbst regulär, weil ja $d(\alpha)$ dann sicher p in möglichst niedriger Potenz enthält. Aber auch falls p ein Teiler der Diskriminante $d(\alpha)$ sein sollte, kann α regulär sein, wenn p in $d(\alpha)$ nicht öfter auftritt, als in der Körperdiskriminante; im entgegengesetzten Falle kann man aber innerhalb $K(\alpha)$ stets eine andere für p reguläre Zahl γ finden, es sei denn daß p ein gemeinsamer außerwesentlicher Teiler aller Gleichungsdiskriminanten von $K(\alpha)$ ist. Wie man dieselbe Aufgabe auch in diesem letzten Falle, also für jede Primzahl p ohne Ausnahme mit Hilfe der Fundamentalgleichung löst, wird sich im nächsten Paragraphen mit Hilfe der jetzt durchzuführenden Betrachtungen leicht ergeben.

Es sei also p eine beliebige reelle Primzahl,

$$(1) \qquad p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_h^{e_h}$$

ihre Zerlegung innerhalb $K(\alpha)$, und es sei wieder allgemein f_i der Grad von $\mathfrak{p}_i$. Ich bezeichne mit $\mathfrak{p}$ irgend einen unter diesen h Primfaktoren, und mit e und f seine Ordnung und seinen Grad. Ist dann γ eine für den Bereich von p reguläre ganze algebraische Zahl, so besitzen die ef zu $\mathfrak{p}$ gehörigen, zu γ konjugierten Zahlen:

$$(2) \qquad \begin{matrix} \gamma_1, & \gamma_2, & \ldots \gamma_e \\ \gamma_1^{(p)}, & \gamma_2^{(p)}, & \ldots \gamma_e^{(p)} \\ \cdot & \cdot & \cdot \\ \gamma_1^{(p^{f-1})}, & \gamma_2^{(p^{f-1})}, & \ldots \gamma_e^{(p^{f-1})}. \end{matrix}$$

die folgenden Entwicklungen für den Bereich von p

$$\text{(2a)}\quad \begin{aligned} \gamma_i \;\; &= \eta_0 + \eta_1 \pi_i + \eta_2 \pi_i^2 + \eta_3 \pi_i^3 + \cdots \\ \vdots \;\;\; & \quad \cdots\cdots\cdots\cdots \\ \gamma_i^{(p^{f-1})} &= \eta_0^{p^{f-1}} + \eta_1^{p^{f-1}} \pi_i^{(p^{f-1})} + \eta_2^{p^{f-1}} \left(\pi_i^{(p^{f-1})}\right)^2 + \cdots \end{aligned} \qquad (i = 1, 2, \ldots e)$$

Die Anfangsglieder aller konjugierten Zahlen der ersten, zweiten, $\ldots f^{\text{ten}}$ Reihe sind die Einheitswurzeln:

$$\eta_0, \; \eta_0^p, \; \ldots \eta_0^{p^{f-1}},$$

und sie sind nach der über γ gemachten Voraussetzung voneinander und von den Anfangsgliedern aller zu den übrigen Primteilern gehörigen konjugierten Zahlen verschieden; endlich sind die zweiten Koeffizienten $\eta_1^{p^k}$ alle von Null verschieden.

Für jede dieser ef konjugierten Zahlen $\gamma_i^{(p^k)}$ modulo $\mathfrak{p}$ gilt dann die Kongruenz:

$$\gamma_i^{(p^k)} \equiv \eta_0^{p^k} \pmod{\mathfrak{p}};$$

bildet man also jetzt das Produkt derjenigen Linearfaktoren, welche zu dem Primteiler $\mathfrak{p}$ gehören, so besteht für ein variables x die Kongruenz:

$$\text{(3)}\qquad \prod_{i=1}^{e} \prod_{k=0}^{f-1} (x - \gamma_i^{(p^k)}) \equiv \prod_{i=1}^{e} \prod_{k=0}^{f-1} (x - \eta_0^{p^k}) \equiv \mathfrak{F}(x)^e \pmod{\mathfrak{p}},$$

wo

$$\text{(3a)}\qquad \mathfrak{F}(x) = (x - \eta_0)(x - \eta_0^p) \cdots (x - \eta_0^{p^{f-1}})$$

eine ganze Funktion f^{ten} Grades von x mit rationalen p-adischen Koeffizienten bedeutet, welche auch modulo p betrachtet irreduktibel ist, weil das Anfangsglied η_0 n. d. V. zu dem Exponenten f selber paßt. Beachtet man, daß die linke Seite dieser Kongruenz als symmetrische Funktion der ef zu $\mathfrak{p}$ gehörigen konjugierten Zahlen $\gamma_i^{(p^k)}$ ebenfalls eine ganze Funktion mit rationalen p-adischen Koeffizienten ist, so kann die Kongruenz (3) nur dann modulo $\mathfrak{p}$ erfüllt sein, wenn sie auch für die reelle Primzahl p als Modul besteht.

Bezeichnen wir jetzt also allgemein das Produkt aller $e_i f_i$ zu einem der h Primfaktoren $\mathfrak{p}_i$ gehörigen Linearfaktoren durch $F_i(x)$, und das Produkt

$$(x - \overset{(i)}{\eta}_0)(x - \overset{(i)}{\eta}_0{}^{p}) \cdots (x - \overset{(i)}{\eta}_0{}^{p^{f-1}})$$

der f_i zu den entsprechenden Anfangsgliedern gehörigen Linearfaktoren durch $\mathfrak{F}_i(x)$, so ergeben sich zunächst die folgenden h Kongruenzen:

$$\text{(4)}\qquad F_i(x) \equiv \mathfrak{F}_i(x)^{e_i} \pmod{p} \qquad (i = 1, 2, \ldots h),$$

und durch Multiplikation jener h Kongruenzen erhält man endlich die folgende wichtige Zerlegung:

(5) $$F(x) = F_1(x) F_2(x) \cdots F_h(x) \equiv \mathfrak{F}_1(x)^{e_1} \mathfrak{F}_2(x)^{e_2} \cdots \mathfrak{F}_h(x)^{e_h} \pmod{p}$$

wo $F(x)$ eben die linke Seite der irreduktiblen Gleichung n^{ten} Grades bedeutet, welcher γ nebst seinen n konjugierten genügt.

Die h Funktionen $\mathfrak{F}_i(x)$ sind nicht nur für den Bereich von p, sondern auch modulo p betrachtet irreduktibel, d. h. ihre nullten Näherungswerte $\mathfrak{F}_i^{(0)}(x)$ sind modulo p unzerlegbar; sie sind ferner alle modulo p inkongruent, da anderenfalls γ nicht regulär wäre. Jede von diesen h Funktionen $\mathfrak{F}_i(x)$ ist einem der h Primfaktoren $\mathfrak{p}_i$ eindeutig zugeordnet, und zwar ist ihr Grad f_i gleich dem Grade von $\mathfrak{p}_i$, und der Exponent e_i der in $F(x)$ enthaltenen Potenz von $\mathfrak{F}_i(x)$ gleich der Ordnung des zugeordneten Primteilers.

Um nun weiter die enge Beziehung zwischen diesen Funktionen und den zugeordneten Primfaktoren darzulegen, stelle ich die folgende einfache Betrachtung an: Es sei wieder $\mathfrak{p}$ einer der h Primfaktoren, und

$$\mathfrak{F}(x) = (x - \eta_0)(x - \eta_0^p) \cdots (x - \eta_0^{p^{f-1}})$$

die zugeordnete Funktion. Substituiert man nun für x zunächst irgend eine der ef zu $\mathfrak{p}$ gehörigen Zahlen $\gamma_i^{(p^k)}$, etwa γ_1, so ergibt sich:

$$\mathfrak{F}(\gamma_1) = (\gamma_1 - \eta_0)(\gamma_1 - \eta_0^p) \cdots (\gamma_1 - \eta_0^{p^{f-1}}) \equiv 0 \pmod{\mathfrak{p}},$$

weil sich in der einen Differenz $\gamma_1 - \eta_0$ das Anfangsglied η_0 forthebt. Da aber in dieser Differenz

$$\gamma_1 - \eta_0 = \eta_1 \pi_1 + \cdots$$

das Anfangsglied η_1 n. d. V. nicht Null ist, und da die Anfangsglieder $\eta_0 - \eta_0^{p^k}$ aller übrigen Differenzen $\gamma_1 - \eta_0^{p^k}$ $\mathfrak{p}$ gar nicht enthalten, so ist $\mathfrak{F}(\gamma_1)$ auch nur durch die erste Potenz von $\mathfrak{p}$ teilbar, d. h. es bestehen die Kongruenzen:

(6) $$\mathfrak{F}(\gamma_1) \equiv 0 \pmod{\mathfrak{p}}, \quad \mathfrak{F}(\gamma_1) \gtrless 0 \pmod{\mathfrak{p}^2}.$$

Substituiert man dagegen in $\mathfrak{F}(x)$ für x eine zu einem anderen Primteiler $\mathfrak{p}'$ gehörige Wurzel γ_1', so ergibt sich

(6a) $$\mathfrak{F}(\gamma_1') \gtrless 0 \pmod{\mathfrak{p}'},$$

denn andernfalls hätten ja die beiden zu $\mathfrak{p}$ und $\mathfrak{p}'$ gehörigen modulo p irreduktibeln Funktionen $\mathfrak{F}(x)$ und $\mathfrak{F}'(x)$ modulo $\mathfrak{p}'$, also auch modulo p einen gemeinsamen Teiler, wären also für diesen Modul kongruent.

Die h p-adischen ganzen algebraischen Zahlen

$$(7) \qquad \mathfrak{F}_1(\gamma), \quad \mathfrak{F}_2(\gamma), \ldots \mathfrak{F}_h(\gamma)$$

haben also die Eigenschaft, daß allgemein

$$(7\text{a}) \qquad \bar{\pi}_i = \mathfrak{F}_i(\gamma)$$

durch den zugeordneten Primteiler $\mathfrak{p}_i$ genau einmal teilbar ist, aber keinen der $(h-1)$ übrigen Primteiler $\mathfrak{p}_k$ enthält; jene h Zahlen sind also Primzahlen bzw. für den Bereich von $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_h$.

Hieraus folgt, daß man die Zerlegung der reellen Primzahl p in ihre Primfaktoren vollständig beherrscht, sobald man nur die in der Kongruenz (5) auftretenden irreduktiblen Funktionen $\mathfrak{F}_i(x)$ finden kann; denn diese liefern uns die Ordnung e_i und den Grad f_i eines jeden von diesen Primteilern, sowie eine zugehörige Primzahl $\bar{\pi}_i = \mathfrak{F}_i(\gamma)$. Aber gerade zur Bestimmung jener Faktoren $\mathfrak{F}_i(x)$ braucht man ja die Entwicklung der konjugierten Zahlen γ nach ganzen oder gebrochenen Potenzen von p, und diese setzt ihrerseits wieder die Kenntnis der Primfaktoren von p voraus.

Jene h Funktionen (7) verlieren nun ihre wesentlichen Eigenschaften nicht, wenn man sie durch ihre nullten Näherungswerte modulo p

$$(7\text{b}) \qquad \mathfrak{F}_1^{(0)}(x), \quad \mathfrak{F}_2^{(0)}(x), \ldots \mathfrak{F}_h^{(0)}(x)$$

ersetzt, und diese sind modulo p irreduktible ganze Funktionen mit gewöhnlichen ganzzahligen Koeffizienten, welche man aus der Grundgleichung $F(x)$ ohne weitere Vorkenntnisse durch eine endliche Anzahl von Versuchen finden kann. In der Tat hängt ja jede Funktion $\mathfrak{F}_i(x)$ mit ihrem nullten Näherungswerte durch eine Gleichung

$$(8) \qquad \mathfrak{F}_i^{(0)}(x) = \mathfrak{F}_i(x) - p\bar{\mathfrak{F}}_i(x)$$

zusammen, wo $\bar{\bar{\mathfrak{F}}}_i(x)$ eine ganze Funktion von niedrigerem als dem f_i^{ten} Grade mit ganzen p-adischen Koeffizienten bedeutet. Ersetzt man nun in der Kongruenz (5) die Funktionen $\mathfrak{F}_i(x)$ durch die ihnen kongruenten $\mathfrak{F}_i^{(0)}(x)$, so folgt:

$$(9) \qquad F(x) \equiv \mathfrak{F}_1^{(0)}(x)^{e_1}\mathfrak{F}_2^{(0)}(x)^{e_2} \ldots \mathfrak{F}_h^{(0)}(x)^{e_h} \pmod{p},$$

und diese Kongruenz liefert die Zerlegung der Funktion $F(x)$ in ihre modulo p irreduktiblen ganzzahligen Faktoren, welche nach dem a. S. 77 bewiesenen Satze eindeutig bestimmt ist und durch eine endliche Anzahl von Versuchen gefunden werden kann.

Ferner haben die Näherungswerte (7b) auch die erste in der Kongruenz (6) und die in (6a) ausgedrückte Eigenschaft. Substituiert

man nämlich für x in der Gleichung (8) das eine Mal eine zu $\mathfrak{p}_i$ gehörige Zahl γ_i, das andere Mal eine zu einem anderen Primteiler $\mathfrak{p}_k$ zugeordnete γ_k und betrachtet sie das eine Mal modulo $\mathfrak{p}_i$, das andere modulo $\mathfrak{p}_k$, so folgen aus (6) und (6a) die beiden Kongruenzen:

$$\begin{aligned} \mathfrak{F}_i^{(0)}(\gamma_i) &\equiv \mathfrak{F}_i(\gamma_i) \equiv 0 \pmod{\mathfrak{p}_i} \\ \mathfrak{F}_i^{(0)}(\gamma_k) &\equiv \mathfrak{F}_i(\gamma_k) \gtrless 0 \pmod{\mathfrak{p}_k}. \end{aligned} \tag{10}$$

Ist ferner $\mathfrak{p}_i$ ein Primteiler von p, dessen Ordnung e_i größer als Eins ist, so ist auch die zweite für $\mathfrak{F}_i(x)$ geltende Kongruenz in (6) für den Näherungswert $\mathfrak{F}_i^{(0)}(x)$ erfüllt; da dann nämlich p mindestens durch $\mathfrak{p}_i^2$ teilbar ist, so liefert die Substitution $x = \gamma_i$ in jene Kongruenz (8) für den Modul $\mathfrak{p}_i^2$ die Beziehung:

$$\mathfrak{F}_i^{(0)}(\gamma_i) \equiv \mathfrak{F}_i(\gamma_i) \gtrless 0 \mod \mathfrak{p}_i^2. \tag{10a}$$

In diesem Falle hat also auch der nullte Näherungswert $\mathfrak{F}_i^{(0)}(x)$ die Eigenschaft, daß die gewöhnliche algebraische Zahl:

$$\pi_i^{(0)} = \mathfrak{F}_i^{(0)}(\gamma)$$

durch den zugehörigen Primteiler $\mathfrak{p}_i$ einmal und nur einmal, durch die übrigen Primteiler $\mathfrak{p}_k$ aber gar nicht teilbar ist.

Nur in dem Falle, wo p den Primteiler $\mathfrak{p}_i$ einfach enthält, könnte die Zahl $\mathfrak{F}_i^{(0)}(\gamma)$ durch $\mathfrak{p}_i^2$ teilbar sein, während $\mathfrak{F}_i(\gamma)$ nur die erste Potenz von p enthält; denn dann sind ja $\mathfrak{F}_i(\gamma)$ und $\mathfrak{F}_i^{(0)}(\gamma)$ nach (8) nicht modulo $\mathfrak{p}_i^2$, sondern nur modulo $\mathfrak{p}_i$ kongruent. Ob dieser Ausnahmefall zufällig eintritt oder nicht, erkennt man ohne weiteres durch die Bildung der Norm von $\mathfrak{F}_i^{(0)}(\gamma)$; denn da diese Zahl außer $\mathfrak{p}_i$ überhaupt keinen Primteiler von p enthält, so ist $n\,(\mathfrak{F}_i^{(0)}(\gamma))$ dann und nur dann genau durch $n\,(\mathfrak{p}_i) = p^{f_i}$ teilbar, wenn $\mathfrak{F}_i^{(0)}(\gamma)$ genau durch $\mathfrak{p}_i$ divisibel ist, während anderenfalls jene Norm mindestens die Potenz $n\,(\mathfrak{p}_i^2) = p^{2f_i}$ enthalten würde, in welcher der Exponent f_i gleich dem Grade von $\mathfrak{F}_i^{(0)}(x)$ ist. Sollte nun die Bildung der Norm ergeben, daß $\mathfrak{F}_i^{(0)}(\gamma)$ durch $\mathfrak{p}_i^2$ teilbar ist, so ist sicher

$$\pi_i^{(0)} = p + \mathfrak{F}_i^{(0)}(\gamma)$$

eine gewöhnliche ganze algebraische Zahl von $K(\alpha)$, welche durch $\mathfrak{p}_i$ nur einmal teilbar ist und keinen anderen Divisor $\mathfrak{p}_k$ enthält, denn es ist ja dann

$$\begin{aligned} \pi_i^{(0)} &\equiv \mathfrak{F}_i^{(0)}(\gamma) \equiv 0 \quad \mod \mathfrak{p}_i \\ \pi_i^{(0)} &\equiv \mathfrak{F}_i^{(0)}(\gamma) \gtrless 0 \quad \mod \mathfrak{p}_k; \end{aligned} \tag{10b}$$

und endlich ist $\pi_i^{(0)}$ nicht durch $\mathfrak{p}_i^2$ teilbar, weil n. d. V. $\mathfrak{F}_i^{(0)}(\gamma)$ jenen Teiler zweimal enthält, während er in p nur einmal auftritt.

Die soeben durchgeführte Betrachtung gibt uns nun ein Mittel, jeden der h Primteiler $\mathfrak{p}_i$ von p völlig rein, nämlich als den größten gemeinsamen Teiler von zwei ganzen Zahlen darzustellen. Ist nämlich $\mathfrak{F}_i^{(0)}(x)$ wieder die zu $\mathfrak{p}_i$ gehörige irreduktible Funktion, so besteht in jedem Falle die Gleichung

$$\mathfrak{p}_i = \left(p,\ \mathfrak{F}_i^{(0)}(\gamma)\right), \tag{11}$$

d. h. $\mathfrak{p}_i$ ist der größte gemeinsame Teiler der zu $\mathfrak{p}_i$ gehörigen Primzahl p und der ganzen algebraischen Zahl $\mathfrak{F}_i^{(0)}(\gamma)$. In der Tat ist zunächst ein nicht zu p gehöriger Primteiler $\mathfrak{q}$ nicht gemeinsamer Teiler jener beiden Zahlen, da er nicht in p enthalten ist, ebensowenig ist ein von $\mathfrak{p}_i$ verschiedener zu p gehöriger Primteiler $\mathfrak{p}_k$ ein Teiler jener beiden Zahlen, denn er ist ja nicht in $\mathfrak{F}_i^{(0)}(\gamma)$ enthalten. Endlich ist $\mathfrak{p}_i$ sicher einmal in beiden Zahlen enthalten, aber nicht zweimal; denn tritt $\mathfrak{p}_i$ zweimal in p auf, so ist $\mathfrak{F}_i^{(0)}(\gamma)$ nach dem oben geführten Beweise genau durch die erste Potenz von p teilbar; im anderen Falle kommt $\mathfrak{p}_i$ eben sicher nur einmal in p vor. Wir können also jetzt den folgenden wichtigen Satz aussprechen:

Es sei γ eine für den Bereich von p reguläre Zahl, und

$$F(x) = 0$$

die Gleichung, der sie genügt. Ist dann:

$$F(x) \equiv \mathfrak{F}_1^{(0)}(x)^{e_1}\,\mathfrak{F}_2^{(0)}(x)^{e_2}\cdots\mathfrak{F}_h^{(0)}(x)^{e_h} \pmod{p} \tag{12}$$

die Zerlegung der Funktion $F(x)$ in ihre modulo p irreduktiblen Faktoren, so ist

$$p = \left(p,\ \mathfrak{F}_1^{(0)}(\gamma)\right)^{e_1}\left(p,\ \mathfrak{F}_2^{(0)}(\gamma)\right)^{e_2}\cdots\left(p,\ \mathfrak{F}_h^{(0)}(\gamma)\right)^{e_h} \tag{12a}$$

die Zerlegung dieser Primzahl in ihre Primfaktoren. Allgemein besitzt der zu $\mathfrak{F}_i^{(0)}(x)$ gehörige Primteiler

$$\mathfrak{p}_i = \left(p,\ \mathfrak{F}_i^{(0)}(\gamma)\right) \tag{12b}$$

den Grad f_i und die Ordnung e_i, wenn die irreduktible Funktion $\mathfrak{F}_i^{(0)}(x)$ den Grad f_i hat, und modulo p betrachtet ein e_i-facher Teiler von $F(x)$ ist.

Mit Hilfe dieses Satzes gestaltet sich die Zerlegung derjenigen reellen Primzahlen, welche z. B. nicht in der Diskriminante der Grundgleichung

aufgehen, ganz wunderbar einfach. Ich zeige dies an der vorher betrachteten Gleichung:

(13) $$F(x) = x^3 - x^2 - 2x - 8 = 0.$$

Die soeben auseinandergesetzte Methode kann hier zur Dekomposition aller Primzahlen p, außer der Zahl 2, angewendet werden, da sie allein außerwesentlicher Teiler der Gleichungsdiskriminante $-4 \cdot 503$ ist; und man braucht dazu allein die Zerlegung der Funktion $F(x)$ in ihre modulo p irreduktiblen ganzzahligen Faktoren. Da diese Funktion dann und nur dann überhaupt modulo p zerfällt, wenn sie mindestens einen ganzzahligen Linearfaktor besitzt, so braucht man für jede Primzahl p nur zu untersuchen, ob $F(i)$ für $i = 0, \pm 1, \pm 2, \cdots, \pm \frac{p-1}{2}$ durch p teilbar ist. So ergibt eine einfache Rechnung, daß jene Funktion z. B. modulo 3, 7, 11, 13, 23 unzerlegbar ist, während für die Primzahlen 5, 17, 19 die folgenden Zerlegungen in irreduktible Faktoren bestehen:

(14) $$\begin{aligned} x^3 - x^2 - 2x - 8 &\equiv (x-1)(x^2-2) \pmod{5} \\ &\equiv (x-7)(x^2+6x+6) \pmod{17} \\ &\equiv (x+3)(x^2-4x+10) \pmod{19}. \end{aligned}$$

In dem zu der Gleichung (13) gehörigen Körper $K(\alpha)$ sind also 3, 7, 11, 13, 23 selbst Primzahlen; dagegen zerfallen 5, 17 und 19 in je einen Primfaktor ersten und einen zweiten Grades, und zwar ist:

(14a) $$\begin{aligned} 5 &= (5,\ \alpha - 1)(5,\ \alpha^2 - 2) \\ 17 &= (17,\ \alpha - 7)(17,\ \alpha^2 + 6\alpha + 6) \\ 19 &= (19,\ \alpha + 3)(19,\ \alpha^2 - 4\alpha + 10). \end{aligned}$$

Sehr leicht ergeben sich so auch weiter die Zerlegungen der Primzahlen des ersten Hundert. Da endlich die Primzahl 503 in der Diskriminante von $F(x)$ nur einmal enthalten ist, so folgt leicht aus den Bemerkungen a. S. 231 unten, daß für den Modul 503 die folgende Zerlegung von $F(x)$ bestehen muß:

$$F(x) \equiv (x-a)^2(x-b) \pmod{503}.$$

Der erste Linearfaktor $x - a$ ergibt sich als der größte gemeinsame Teiler von $F(x)$ und $F'(x)$ modulo 503:

$$(x^3 - x^2 - 2x - 8,\ 3x^2 - 2x - 2) = x + \tfrac{37}{7},$$

und durch Substitution des Wertes $a = -\frac{37}{7}$ erhält man leicht durch Koeffizientenvergleichung $b = \frac{81}{7}$; es ist also:

(14b) $$x^3 - x^2 - 2x - 8 \equiv (x + \tfrac{37}{7})^2 (x - \tfrac{81}{7}) \pmod{503},$$

und hieraus folgt für 503 die Zerlegung in Primfaktoren:

(14c) $$503 = (503,\ \alpha + \tfrac{37}{7})^2 (503,\ \alpha - \tfrac{81}{7}).$$

§ 2. Die Zerlegung der Fundamentalgleichung für eine reelle Primzahl als Modul.

Aus dem im vorigen Abschnitte behandelten Beispiele ergibt sich, daß für fast alle reellen Primzahlen die Zerlegung in ihre Primteiler innerhalb eines Körpers $K(\alpha)$ höchst einfach durchgeführt werden kann. Ist dagegen die betreffende Primzahl p ein gemeinsamer außerwesentlicher Diskriminantenteiler von $K(\alpha)$, so reicht die soeben auseinandergesetzte Methode nicht aus, da man ja in diesem Falle keine Grundgleichung finden kann, welche p nicht als außerwesentlichen Teiler enthielte. Es soll daher jetzt eine Vorschrift gegeben werden, mit deren Hilfe das Fundamentalproblem, eine beliebige Primzahl innerhalb eines beliebigen Körpers in ihre Primteiler zu zerlegen, vollständig ohne jede Ausnahmefälle gelöst wird. Sie beruht auf der a. S. 270 unten bewiesenen Tatsache, daß die Diskriminante $D(u_1, \ldots, u_n)$ der Fundamentalgleichung für unbestimmte u_i allein durch die Körperdiskriminante teilbar ist, also keine außerwesentlichen Teiler enthält. Hieraus folgt, daß die Fundamentalform:

$$(1) \qquad w = u_1 \xi^{(1)} + u_2 \xi^{(2)} + \cdots + u_n \xi^{(n)}$$

für unbestimmte $u_1, u_2, \ldots u_n$ in bezug auf jede reelle Primzahl den Charakter einer regulären Zahl haben wird. Zerlegt man also die linke Seite der Fundamentalgleichung, der die Form w nebst ihren n konjugierten genügt, für unbestimmte u_i in ihre modulo p irreduktiblen Faktoren, so ist anzunehmen, daß diese uns stets die Primfaktoren von p in derselben Weise liefern werden, wie dies im vorigen Paragraphen bei den irreduktiblen Faktoren $\mathfrak{F}_i^{(0)}(x)$ der Fall war, welche sich aus der Zerlegung der linken Seite der Gleichung für die modulo p reguläre Zahl γ ergaben. Dies ist nun wirklich der Fall, und der Beweis wird ganz analog wie a. a. O. geführt; ich brauche daher nur das wesentlich Neue hervorzuheben.

Es sei (1) die Fundamentalform des Körpers $K(\alpha)$ und

$$(2) \qquad p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_h^{e_h}$$

die Zerlegung der zu untersuchenden reellen Primzahl innerhalb dieses Körpers. Es bedeute nun $\mathfrak{p}$ einen dieser h Primfaktoren, e und f seien seine Ordnung und sein Grad. Dann bezeichne ich wie a. S. 298 (2) durch:

$$(3) \qquad \begin{matrix} w_1, & w_2, & \ldots w_e \\ w_1^{(p)}, & w_2^{(p)}, & \ldots w_e^{(p)} \\ \vdots & & \\ w_1^{(p^{f-1})}, & w_2^{(p^{f-1})}, & \ldots w_e^{(p^{f-1})} \end{matrix}$$

die ef zu $\mathfrak{p}$ gehörigen konjugierten Fundamentalformen. Denkt man sich diese für den Bereich von $\mathfrak{p}$ nach Potenzen einer zugehörigen Primzahl π entwickelt, so erhält man wie a. S. 299 in (2a) die folgenden Reihen:

$$
(3\text{a})\quad
\begin{aligned}
w_i &= U_0 + U_1\pi_i + U_2\pi_i^2 + \cdots \\
w_i^{(p)} &= U_0^{(p)} + U_1^{(p)}\pi_i^{(p)} + U_2^{(p)}\left(\pi_i^{(p)^2}\right) + \cdots \\
&\vdots \\
w_i^{(p^{f-1})} &= U_0^{(p^{f-1})} + U_1^{(p^{f-1})}\pi_i^{(p^{f-1})} + U_2^{(p^{f-1})}\left(\pi_i^{(p^{f-1})^2}\right) + \cdots, \\
& (i = 1, 2, \ldots e)
\end{aligned}
$$

wo $U_0, U_1, \ldots U_0^{(p)}, U_1^{(p)}, \ldots$ Linearformen der Unbestimmten $u_1, u_2, \ldots u_n$ bedeuten, deren Koeffizienten konjugierte Zahlen des Koeffizientenkörpers $K(\eta)$ sind.

Alle diese ef Entwicklungen sind nun für den Modul $\mathfrak{p}$ bzw. kongruent ihren Anfangsgliedern:

$$U_0,\ U_0^{(p)}, \ldots U_0^{(p^{f-1})},$$

und je e Formen, welche in (3) in derselben Zeile stehen, besitzen dasselbe Anfangsglied. Hieraus folgt, daß für die linke Seite der zu $\mathfrak{p}$ gehörigen Fundamentalgleichung, d. h. für das Produkt der ef Linearfaktoren $\bar{w} - w_i^{(p^k)}$ modulo $\mathfrak{p}$ die folgende Kongruenz für ein variables $\bar{w}$ und für unbestimmte u_i besteht:

$$(3\text{b})\qquad \prod_{i,k}\left(\bar{w} - w_i^{(p^k)}\right) \equiv \mathfrak{F}(\bar{w})^e \pmod{\mathfrak{p}},$$

wenn wieder wie a. S. 299 (3a)

$$(4)\qquad \mathfrak{F}(\bar{w}) = (\bar{w} - U_0)\left(\bar{w} - U_0^{(p)}\right)\cdots\left(\bar{w} - U_0^{(p^{f-1})}\right)$$

das Produkt der zu den Anfangsgliedern gehörigen Linearfaktoren bedeutet.

Auf beiden Seiten der Kongruenz (3b) modulo $\mathfrak{p}$ steht je eine ganze Funktion der $(n+1)$ Variablen $\bar{w}, u_1, \ldots u_n$ mit rationalen p-adischen Koeffizienten; also muß sie auch modulo p selbst erfüllt sein. Ferner ist die rechts stehende Funktion $\mathfrak{F}(\bar{w}, u_i)$ modulo p betrachtet für unbestimmte u_i irreduktibel, denn sie geht für alle ganzzahligen Spezialisierungen $u_i = a_i$ in die entsprechenden Funktionen f^{ten} Grades $\mathfrak{F}(\bar{w})$ a. S. 299 (3a) über, denen alle Zahlen des Körpers $K(\alpha)$ modulo $\mathfrak{p}$ betrachtet genügen. Zerfiele also $\mathfrak{F}(\bar{w}, u_i)$ für unbestimmte u_i, so müßte dasselbe für jede Funktion $\mathfrak{F}(x)$ der Fall sein, welche zu

einer Zahl des Körpers $K(\alpha)$ gehört, während doch ganze Zahlen existieren, welche zum Exponenten f selbst passen, also modulo $\mathfrak{p}$ betrachtet irreduktiblen Kongruenzen des f^{ten} Grades genügen.

Denkt man sich nun für alle h Primfaktoren $\mathfrak{p}_i$ die zugehörigen Fundamentalgleichungen $F_i(\overline{w}) = 0$ gebildet und ihre linken Seiten dann auf die in (3b) angegebene Weise modulo p in der Form $\mathfrak{F}_i(\overline{w}, u_k)^e$ dargestellt, so sind diese alle modulo p inkongruent, da sonst dieselben Funktionen auch für jede ganzzahlige Spezialisierung der u_i kongruent sein müßten, und es ergibt sich endlich für die linke Seite der ganzen Fundamentalgleichung folgende Zerlegung in modulo p irreduktible p-adische Faktoren:

(5) $$F(\overline{w}, u_k) \equiv \mathfrak{F}_1(\overline{w}, u_k)^{e_1}\,\mathfrak{F}_2(\overline{w}, u_k)^{e_2} \ldots \mathfrak{F}_h(\overline{w}, u_k)^{e_h} \pmod{p},$$

entsprechend der Zerfällung der Primzahl p

(5a) $$p = \mathfrak{p}_1^{e_1}\,\mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_h^{e_h}$$

in ihre Primfaktoren.

Man erkennt nun ohne weiteres, daß die zu einem Primdivisor $\mathfrak{p}$ gehörige Funktion

$$\mathfrak{F}(\overline{w}, u_k) = (\overline{w} - U_0)\left(\overline{w} - U_0^{(p)}\right) \cdots \left(\overline{w} - U_0^{(p^f - 1)}\right)$$

für unbestimmte u_k ein einziges Mal durch $\mathfrak{p}$ teilbar wird, wenn $\overline{w}$ gleich der Fundamentalform w in (1) gesetzt wird, daß sie aber keinen anderen Primteiler $\mathfrak{p}'$ enthält. Ersetzt man nämlich in (4) $\overline{w}$ durch eine der ef zu $\mathfrak{p}$ gehörigen Entwicklungen, etwa durch w_i in (3a), so erkennt man genau wie a. S. 300 Mitte, daß $\mathfrak{F}(w_i, u_k)$ ein einziges Mal durch $\mathfrak{p}$ teilbar wird, weil sich nur in dem einen Linearfaktor $w_i - U_0$ das Anfangsglied forthebt, während der Koeffizient U_1 von π_i von Null verschieden ist. Substituiert man dagegen in (4) für $\overline{w}$ eine zu einem anderen Primteiler $\mathfrak{p}'$ gehörige Entwicklung w', so ist in dem Produkte:

$$\mathfrak{F}(w', u_k) = (w' - U_0)\left(w' - U_0^{(p)}\right) \cdots \left(w' - U_0^{(p^f - 1)}\right)$$

kein einziger Faktor für unbestimmte u_i durch $\mathfrak{p}'$ teilbar, denn sonst hätten ja $\mathfrak{F}(\overline{w}, u_k)$ und die zu $\mathfrak{p}'$ gehörige Funktion $\mathfrak{F}'(\overline{w}, u_k)$ für unbestimmte u_i einen gemeinsamen durch das Euklidische Teilerverfahren bestimmbaren rationalen Teiler modulo p; sie wären also entweder modulo p zerlegbar oder identisch. Auch hier sind also die h p-adischen algebraischen Formen

(6) $$\overline{\pi}_i = \mathfrak{F}_i(w, u_k)$$

Primfunktionen für den Bereich des entsprechenden Divisors $\mathfrak{p}_i$, und sie sind durch keinen der $h - 1$ übrigen Primteiler teilbar.

Dieselben Eigenschaften besitzen im wesentlichen auch die nullten Näherungswerte $\mathfrak{F}_i^{(0)}(\overline{w}, u_k)$ jener Funktionen $\mathfrak{F}_i(\overline{w}, u_k)$, welche also ganze Funktionen von $\overline{w}, u_1, \ldots u_n$ mit Zahlenkoeffizienten der Reihe $0, 1, \ldots p-1$ sind, und sich aus der eindeutig bestimmten Zerlegung der Fundamentalgleichung

$$(7) \qquad F(\overline{w}, u_k) \equiv \mathfrak{F}_1^{(0)}(\overline{w}, u_k)^{e_1} \cdots \mathfrak{F}_h^{(0)}(\overline{w}, u_k)^{e_h} \pmod{p}$$

in ihre modulo p irreduktiblen ganzzahligen Faktoren direkt ergeben. Da nämlich zwischen einer p-adischen Funktion $\mathfrak{F}_i(\overline{w}, u_k)$ und ihrem nullten Näherungswerte eine Gleichung besteht:

$$(8) \qquad \mathfrak{F}_i^{(0)}(\overline{w}, u_k) = \mathfrak{F}_i(\overline{w}, u_k) - p\,\overline{\mathfrak{F}}_i(\overline{w}, u_k),$$

so folgt genau wie a. S. 301 (8), daß auch $\mathfrak{F}_i^{(0)}(w, u_k)$ für unbestimmte u_k durch den zugehörigen Teiler $\mathfrak{p}_i$ aber durch keinen anderen Divisor von p teilbar ist. Ist ferner $\mathfrak{p}_i$ ein Verzweigungsteiler, also $e_i > 1$, so ist auch $\mathfrak{F}_i^{(0)}(w, u_k)$ sicher nicht durch $\mathfrak{p}_i^2$ teilbar, also $\overline{\pi}_i = \mathfrak{F}_i^{(0)}(w, u_k)$ ebenfalls eine Primzahl für den Bereich von $\mathfrak{p}_i$. Ist dagegen $e_i = 1$, so kann $\mathfrak{F}_i^{(0)}(w, u_k)$ auch jetzt zufällig eine höhere Potenz von $\mathfrak{p}_i$ enthalten. In jedem der beiden Fälle ist aber wieder:

$$(9) \qquad \mathfrak{p}_i = \left(p, \mathfrak{F}_i^{(0)}(w, u_k)\right) \qquad (i = 1, 2, \ldots h).$$

Es ergibt sich also jetzt die folgende ganz allgemeine Vorschrift zur direkten Bestimmung aller Primfaktoren eines beliebigen Körpers $K(\alpha)$:

Es sei $w = u_1 \xi^{(1)} + \cdots + u_n \xi^{(n)}$ eine Fundamentalform für den Körper $K(\alpha)$, und

$$(10) \qquad F(\overline{w}, u_k) = 0$$

die zugehörige Fundamentalgleichung. Um eine beliebige reelle Primzahl p innerhalb $K(\alpha)$ in ihre Primfaktoren zu dekomponieren, zerlege man $F(\overline{w}, u_k)$ für unbestimmte u_k in die modulo p irreduktiblen Faktoren, was stets durch eine endliche Anzahl von Versuchen geschehen kann. Der so sich ergebenden Kongruenz

$$(10\text{a}) \qquad F(\overline{w}, u_k) \equiv \mathfrak{F}_1^{(0)}(\overline{w}, u_k)^{e_1} \cdots \mathfrak{F}_h^{(0)}(\overline{w}, u_k)^{e_h} \pmod{p}$$

entspricht dann die folgende Zerlegung von p in seine Primfaktoren:

$$(10\text{b}) \qquad p = \left(p, \mathfrak{F}_1^{(0)}(w, u_k)\right)^{e_1} \cdots \left(p, \mathfrak{F}_h^{(0)}(w, u_k)\right)^{e_h}.$$

Ist ferner f_i der Grad der irreduktiblen Funktion $\mathfrak{F}_i^{(0)}(\overline{w}, u_k)$,

so besitzt der zugehörige Primteiler $\mathfrak{p}_i$ ebenfalls den Grad f_i und er hat die aus (10a) sich ergebende Ordnung e_i.

Zur vollständigen Darstellung aller Primdivisoren $\mathfrak{p}$ bedarf man also nur der Aufsuchung eines Fundamentalsystemes für $K(\alpha)$ und der Bildung der zugehörigen Fundamentalgleichung; die Zerlegung ihrer linken Seite für alle reellen Primzahlen als Moduln liefert dann alle Primdivisoren ohne jede Ausnahme und jedesmal ihren Grad und ihre Ordnung.

Ich will dieses wichtige Resultat benutzen, um mit seiner Hilfe die noch ausstehende Zerlegung der Primzahl 2 innerhalb des durch die Gleichung

$$(11) \qquad F(\alpha) = \alpha^3 - \alpha^2 - 2\alpha - 8 = 0$$

definierten kubischen Körpers $K(\alpha)$ zu bestimmen, für welchen ja 2 der einzige gemeinsame außerwesentliche Diskriminantenteiler war. Hier bilden die Zahlen $(1, \alpha, \alpha^2)$ kein absolutes Fundamentalsystem, weil ihre Diskriminante $d(\alpha) = -2^2 \cdot 503$ noch den außerwesentlichen Teiler 2, allerdings nur in der zweiten Potenz, enthält. Schreibt man aber die Gleichung (11) in der Form:

$$(12) \qquad \frac{\alpha^2 - \alpha - 2}{2} = \frac{4}{\alpha},$$

und bezeichnet diese beiden einander gleichen Zahlen von $K(\alpha)$ durch β, so erkennt man leicht, daß $\beta = \frac{4}{\alpha}$ eine ganze Zahl ist, denn die Substitution $\alpha = \frac{4}{\beta}$ in (11) lehrt ja, daß β der ganzzahligen Gleichung:

$$G(\beta) = \beta^3 + \beta^2 + 2\beta - 8 = 0$$

genügt. Die drei Zahlen 1, α und $\beta = \frac{\alpha^2 - \alpha - 2}{2}$ bilden nun ein absolutes Fundamentalsystem für $K(\alpha)$, denn offenbar besteht die Determinantengleichung:

$$(13) \qquad |1, \alpha_i, \beta_i|^2 = \left|1, \alpha_i, \frac{\alpha_i^2 - \alpha_i - 2}{2}\right|^2 = \frac{1}{2^2}\,|1, \alpha_i, \alpha_i^2|^2 = -503;$$

jenes ganzzahlige System besitzt also die kleinstmögliche Diskriminante.

Zerlegt man nun die linke Seite der Fundamentalgleichung $F(w) = 0$, der die zu $(1, \alpha, \beta)$ gehörige Fundamentalform:

$$(14) \qquad w = u_0 + u_1\alpha + u_2\beta$$

nebst ihren konjugierten genügt, für unbestimmte u_i in ihre modulo 2 irreduktiblen Linearfaktoren, so ergeben diese nach (10a) die gesuchten Primfaktoren der Primzahl 2.

Aus den a. S. 274 durchgeführten Überlegungen hatte sich bereits ergeben, daß die reelle Primzahl 2 drei verschiedene Primteiler ersten

Grades besitzt, daß also alle drei Wurzeln der Gleichung (11) für den Bereich von 2 rationalen dyadischen Zahlen gleich sind. Eine einfache Diskussion dieser Gleichung zeigt nun, daß die drei konjugierten Wurzeln $\alpha_1, \alpha_2, \alpha_3$ modulo 4 bzw. kongruent 0, 2, 3 sind, und hieraus folgt, daß die entsprechenden zu

$$\beta = \frac{\alpha^2 - \alpha - 2}{2}$$

konjugierten Zahlen $\beta_1, \beta_2, \beta_3$ modulo 2 bzw. kongruent 1, 0, 0 werden. Also sind die drei konjugierten Fundamentalformen $w_i = u_0 + u_1\alpha_i + u_2\beta_i$ für $i = 1, 2, 3$ modulo 2 betrachtet bzw. kongruent

$$(15) \qquad u_0 + 0 \cdot u_1 + u_2, \qquad u_0 + 0 \cdot u_1 + 0 \cdot u_2, \qquad u_0 + u_1 + 0 \cdot u_2.$$

Die linke Seite der Fundamentalgleichung $F(\overline{w}, u_i)$ zerfällt hiernach modulo 2 für unbestimmte u_i in drei rationale Linearfaktoren:

$$(16) \qquad F(\overline{w}, u_i) \equiv (\overline{w} - (u_0 + u_2))\,(\overline{w} - u_0)\,(\overline{w} - (u_0 + u_1)) \pmod 2.$$

Substituiert man also für die Variable $\overline{w}$ die Fundamentalform (14) in (16), so erhält man nach (10b) die folgende Zerlegung von 2

$$(17) \qquad 2 = (2,\ u_1\alpha + u_2(\beta - 1))\,(2,\ u_1\alpha + u_2\beta)\,(2,\ u_1(\alpha - 1) + u_2\beta).$$

Jeder der drei Primteiler von 2 stellt sich also hier als der größte gemeinsame Teiler von 2 und je einer Linearform mit zwei algebraischen Koeffizienten dar. Wir können diese Primteiler auch unter Weglassung der Unbestimmten in der folgenden Form schreiben:

$$(17a) \qquad \begin{aligned} \mathfrak{p}_1 &= (2,\ \alpha,\ \beta - 1) = \left(2,\ \alpha,\ \frac{\alpha^2 - \alpha}{2}\right) \\ \mathfrak{p}_2 &= (2,\ \alpha,\ \beta) \qquad = \left(2,\ \alpha,\ \frac{\alpha^2 - \alpha - 2}{2}\right) \\ \mathfrak{p}_3 &= (2,\ \alpha - 1,\ \beta) = \left(2,\ \alpha - 1,\ \frac{\alpha^2 - \alpha - 2}{2}\right), \end{aligned}$$

denn man erkennt sofort, daß der größte gemeinsame Teiler z. B. der drei Zahlen $(2, \alpha, \beta - 1)$ gleich demjenigen der Zahl 2 und der Form $u\alpha + v(\beta - 1)$ sein muß, weil beide jeden Primteiler gleich oft enthalten. (Vgl. auch die Bemerkungen a. S. 312 Mitte.)

§ 3. Die Darstellung der Divisoren durch algebraische Formen.

In den beiden vorigen Paragraphen wurde gezeigt, wie einfach man jeden Primteiler eines beliebigen Körpers in geschlossener Form darstellen kann, auch wenn er ein Verzweigungsteiler oder ein gemeinsamer außerwesentlicher Diskriminantenteiler des Körpers ist. Ich will diese Resultate benutzen, um nun auch jeden zusammengesetzten ganzen

oder gebrochenen Divisor in ähnlich einfacher Weise wirklich darzustellen. Streng genommen ist für die hier auseinandergesetzte Theorie die explizite Darstellung der Divisoren ebensowenig notwendig, wie in der Riemannschen Theorie der algebraischen Funktionen einer Variablen, da man auch hier nur die Entwickelbarkeit der Zahlen für den Bereich eines Primteilers braucht; die jetzt abzuleitenden Resultate sind aber so interessant und ergeben sich hier so besonders einfach, daß sie doch kurz dargelegt werden sollen.

Ein einfaches Mittel um Divisoren darzustellen, besteht darin, daß man sie als größte gemeinsame Teiler algebraischer Zahlen des Körpers definiert. Sind nämlich $\zeta^{(1)}, \zeta^{(2)}, \ldots \zeta^{(\mu)}$ beliebig viele ganze oder gebrochene Zahlen von $K(\alpha)$, so ist ihr größter gemeinsamer Teiler

(1) $$\mathfrak{D} = (\zeta^{(1)}, \zeta^{(2)}, \ldots \zeta^{(\mu)})$$

derjenige algebraische Divisor, welcher einen jeden Primteiler $\mathfrak{p}$ so oft enthält, als er in den μ Zahlen $\zeta^{(i)}$ mindestens auftritt. Ist also $\mathfrak{p}^r$ die in $\mathfrak{D}$ enthaltene Potenz von $\mathfrak{p}$, so sind alle jene μ Zahlen durch $\mathfrak{p}^r$ teilbar, und mindestens eine unter ihnen enthält auch keine höhere Potenz von $\mathfrak{p}$.

Ist

(2) $$\mathfrak{E} = (\vartheta^{(1)}, \vartheta^{(2)}, \ldots \vartheta^{(\nu)})$$

irgend ein anderer in gleicher Weise dargestellter Divisor, so besteht für das Produkt jener beiden Divisoren folgende Darstellung:

(3) $$\mathfrak{D}\mathfrak{E} = (\zeta^{(1)}\vartheta^{(1)}, \ldots \zeta^{(i)}\vartheta^{(k)}, \ldots) \qquad \begin{pmatrix} i = 1, 2, \cdots \mu \\ k = 1, 2, \cdots \nu \end{pmatrix},$$

d. h. auch dieses Produkt läßt sich einfach als größter gemeinsamer Teiler algebraischer Zahlen darstellen; ist nämlich wieder $\mathfrak{p}$ ein beliebiger Primteiler, welcher d Male in $\mathfrak{D}$, e Male in $\mathfrak{E}$, also $(d+e)$ Male in $\mathfrak{D}\mathfrak{E}$ enthalten ist, und sind $\zeta^{(i)}$ und $\vartheta^{(k)}$ zwei Zahlen jener beiden Divisoren, welche genau bzw. durch $\mathfrak{p}^d$ und $\mathfrak{p}^e$ teilbar sind, so folgt, daß der in (3) rechts stehende Divisor genau durch $\mathfrak{p}^{d+e}$ teilbar ist, weil dieses sicher für das eine Produkt $\zeta^{(i)}\vartheta^{(k)}$ gilt, während alle anderen mindestens diese Potenz von $\mathfrak{p}$ enthalten. Also enthält der rechts stehende Divisor in der Tat diesen Primteiler $\mathfrak{p}$, also auch jeden anderen, genau so oft, als das Produkt $\mathfrak{D}\mathfrak{E}$, die Richtigkeit der obigen Gleichung ist somit vollständig bewiesen.

In vielen Fällen braucht man nicht alle jene $\mu\nu$ Produkte $\zeta^{(i)}\vartheta^{(k)}$, um durch sie das Divisorenprodukt $\mathfrak{D}\mathfrak{E}$ darzustellen, sondern viele unter ihnen können einfach fortgelassen werden. Speziell erkennt man leicht, daß eine beliebige r^{te} Potenz des Divisors $\mathfrak{D}$ schon durch die einfache Gleichung:

(4) $$\mathfrak{D}^r = (\zeta^{(1)r}, \zeta^{(2)r}, \dots \zeta^{(\mu)r})$$

bestimmt ist; ist nämlich wieder $\mathfrak{p}^d$ die in $\mathfrak{D}$ enthaltene Potenz eines beliebigen Primteilers $\mathfrak{p}$, und ist $\zeta^{(i)}$ genau durch $\mathfrak{p}^d$ teilbar, so sind sowohl $\mathfrak{D}^r$ als $\zeta^{(i)r}$ genau durch $\mathfrak{p}^{rd}$ divisibel, während alle anderen Potenzen $\zeta^{(k)r}$ mindestens dieselbe Potenz von $\mathfrak{p}$ enthalten.

Es fragt sich nun, ob auch umgekehrt jeder Divisor $\mathfrak{D}$ in der Form (1) als größter gemeinsamer Teiler von geeignet gewählten algebraischen Zahlen dargestellt werden kann. Dies ist in der Tat der Fall, und der a. S. 243 bewiesene Satz (1a) gibt uns bereits ein Mittel, diese Aufgabe für einen beliebigen Divisor $\mathfrak{D}$, wenn auch nicht auf die einfachste Weise, zu lösen. Ist nämlich $(\xi^{(1)}, \xi^{(2)}, \dots \xi^{(n)})$ ein Fundamentalsystem für die Multipla dieses Divisors oder für das zugehörige Ideal $\mathfrak{J}(\mathfrak{D})$, so folgt aus diesem Satze, daß einfach:

(5) $$\mathfrak{D} = (\xi^{(1)}, \xi^{(2)}, \dots \xi^{(n)}),$$

daß nämlich jener Divisor der größte gemeinsame Teiler der n ganzen oder gebrochenen Zahlen $\xi^{(i)}$ ist. In der Tat ist ja $\mathfrak{D}$ ein gemeinsamer Teiler jener n Zahlen, weil jede ein Multiplum von $\mathfrak{D}$ ist, aber $\mathfrak{D}$ ist nach eben diesem Satze auch ihr größter gemeinsamer Divisor. Wir haben so also eine allgemeingültige Darstellung aller algebraischen Divisoren gewonnen.

Auch in anderer Weise kann man jeden Divisor $\mathfrak{D}$ in geschlossener Form darstellen, wenn man wieder die Unbestimmten zur Hilfe nimmt; unter der Voraussetzung (5) besteht nämlich die Gleichung:

(5a) $$\mathfrak{D} = u_1\xi^{(1)} + u_2\xi^{(2)} + \cdots + u_n\xi^{(n)},$$

d. h. jener Divisor ist gleich der zu dem Ideale $\mathfrak{J}(\mathfrak{D})$ gehörigen Fundamentalform; in der Tat ist jene Form für unbestimmte u_i durch dieselbe Potenz $\mathfrak{p}^r$ eines beliebigen Primteilers $\mathfrak{p}$ genau teilbar, welche in $\mathfrak{D}$ enthalten ist, da ja nach (5) mindestens eine der n Zahlen $\xi^{(i)}$ genau durch $\mathfrak{p}^r$ teilbar ist, während alle übrigen dieselbe oder eine höhere Potenz von $\mathfrak{p}$ enthalten.

Diese Darstellung der Divisoren durch Linearformen mit algebraischen Koeffizienten will ich nun dadurch verallgemeinern und für die Anwendung brauchbarer machen, daß ich auch algebraische Formen beliebigen Grades mit beliebig vielen Unbestimmten zur Darstellung der Divisoren verwende. Es sei

(6) $$F(v_1, v_2, \cdots v_m) = V_1\zeta^{(1)} + V_2\zeta^{(2)} + \cdots + V_\mu\zeta^{(\mu)}$$

eine Form der m Unbestimmten $v_1, \dots v_m$ mit ganzen oder gebrochenen Zahlen $\zeta^{(i)}$ des Körpers als Koeffizienten, in denen die Größen:

(6a) $$V_i = v_1^{r_1^{(i)}} v_2^{r_2^{(i)}} \cdots v_m^{r_m^{(i)}}$$

beliebige aber untereinander verschiedene Produkte von Potenzen der Unbestimmten v_i mit positiven oder negativen ganzzahligen Exponenten bedeuten. Ist dann wieder:

(6b) $$\mathfrak{F} = (\zeta^{(1)}, \zeta^{(2)}, \ldots \zeta^{(\mu)})$$

der größte gemeinsame Teiler der μ Koeffizienten $\zeta^{(i)}$, enthält also $\mathfrak{F}$ jeden Primteiler $\mathfrak{p}$ so oft, als er mindestens in allen μ Zahlen $\zeta^{(i)}$ vorkommt, so ergibt sich genau wie oben für die Linearformen, daß für unbestimmte v_i

(6c) $$\mathfrak{F} = V_1\zeta^{(1)} + \cdots + V_\mu\zeta^{(\mu)}$$

gesetzt werden kann; der Divisor $\mathfrak{F}$ soll deshalb der Teiler der algebraischen Form $F(v_1, \ldots v_m)$ genannt werden. Ist also wieder $\mathfrak{F}$ ein beliebiger Divisor, $(\xi^{(1)}, \xi^{(2)}, \ldots \xi^{(n)})$ das zugehörige Fundamentalsystem, so besteht neben der Darstellung (5a) die allgemeinere Gleichung:

(6d) $$\mathfrak{F} = V_1\xi^{(1)} + V_2\xi^{(2)} + \cdots + V_n\xi^{(n)},$$

wenn $V_1, \ldots V_n$ beliebige aber voneinander verschiedene Produkte von Potenzen beliebig vieler Unbestimmten $v_1, \ldots v_m$ sind.

Schon im § 1 des dritten Kapitels S. 46 ff. wurden solche Formen in dem trivialen Falle betrachtet, daß sie nur von einer einzigen Variablen x abhängen, daß also die Größen V_i nur verschiedene Potenzen x^i dieser Variablen x sind. Hier wurden die Koeffizienten spezieller als ganze rationale p-adische Zahlen angenommen, und ihr größter gemeinsamer Teiler $\mathfrak{D} = p^\delta$ auch hier als der Zahlenteiler der Funktion $f(x)$ bezeichnet. Der Fundamentalsatz dieser Theorie, daß der Zahlenteiler eines Produktes $f(x)g(x)$ gleich dem Produkte der Zahlenteiler seiner Faktoren ist, konnte hier aus dem Grunde so leicht bewiesen werden, weil wir die Glieder $A_k x^k$ aller Funktionen in einer bestimmten Reihenfolge, nämlich nach dem Grade k der zugehörigen Potenz von x, anordnen konnten. Sind wir imstande, auch die Potenzprodukte $V_1, V_2, \ldots V_\mu$ in einer von mehreren Variablen abhängenden Form $F(v_1, \ldots v_m)$ in eindeutig bestimmter Weise und zwar so zu ordnen, daß das Glied höchster Ordnung des Produktes zweier Formen stets gleich dem Produkte der höchsten Glieder seiner Faktoren ist, so können wir genau auf dieselbe Weise, wie in jenem einfachsten Falle, auch hier den Fundamentalsatz der Formentheorie beweisen:

> Sind $\mathfrak{E}$ und $\mathfrak{F}$ die Teiler zweier Formen $E(v_1, \ldots v_m)$ und $F(v_1, \ldots v_m)$, so besitzt das Produkt $E(v_1, \ldots v_m) \cdot F(v_1, \ldots v_m)$ den Teiler $\mathfrak{E}\mathfrak{F}$.

Eine solche Anordnung dieser Potenzprodukte V von mehreren Veränderlichen kann nun leicht folgendermaßen hergestellt werden: Ich bezeichne zunächst alle überhaupt auftretenden Variablen v in beliebiger aber fester Reihenfolge ein für alle Male durch $v_1, v_2, \ldots v_m$ und ordne jedem Produkte

$$V = v_1^{r_1} v_2^{r_2} \cdots v_m^{r_m}$$

das Exponentensystem

$$(r_i) = (r_1, r_2, \cdots r_m), \tag{7}$$

d. h. das System seiner m ganzzahligen Exponenten (von denen auch gewisse Null sein können), in dieser Reihenfolge zu. Besitzen zwei solche Produkte $V = v_1^{r_1} v_2^{r_2} \cdots v_m^{r_m}$ und $W = v_1^{s_1} v_2^{s_2} \cdots v_m^{s_m}$ die Exponentensysteme (r_i) und (s_i), so haben ihr Produkt VW und ihr Quotient $\frac{V}{W}$ offenbar die Exponentensysteme $(r_i + s_i)$ und $(r_i - s_i)$. Ich stelle nun folgende Definition auf:

> Ein Produkt $V = v_1^{r_1} v_2^{r_2} \cdots v_m^{r_m}$ ist von positiver oder von negativer Ordnung, je nachdem in seinem Exponentensystem $(r_1, r_2, \ldots r_m)$ der erste von Null verschiedene Exponent r_i positiv oder negativ ist.

Hieraus folgt sofort, daß ein Produkt VW sicher von positiver bzw. von negativer Ordnung ist, wenn seine Faktoren V und W beide von positiver bzw. beide von negativer Ordnung sind.

Besitzen ferner zwei Produkte:

$$V = v_1^{r_1} v_2^{r_2} \cdots v_m^{r_m} \quad \text{und} \quad W = v_1^{s_1} v_2^{s_2} \cdots v_m^{s_m}$$

die Exponentensysteme (r_i) und (s_i), so soll die Ordnung von V kleiner als die von W heißen, wenn der Quotient $\frac{V}{W}$ von negativer Ordnung ist, wenn also in seinem Exponentensystem $(r_1 - s_1, r_2 - s_2, \cdots r_m - s_m)$ der erste von Null verschiedene Exponent negativ ist. Sind dann drei solche Produkte U, V und W so geordnet, daß U von höherer Ordnung als V und V von höherer Ordnung als W ist, so ist sicher auch die Ordnung von U größer als die von W, weil unter der gemachten Voraussetzung der Quotient

$$\frac{W}{U} = \frac{W}{V} \cdot \frac{V}{U},$$

als Produkt von zwei Faktoren negativer Ordnung, selbst von negativer Ordnung ist.

Hieraus folgt, daß wir beliebig viele solche Produkte $V_1, V_2, \ldots$ stets so anordnen können, daß die Ordnung jedes folgenden Gliedes

kleiner ist als die jedes vorhergehenden, und so sollen von jetzt ab die Glieder einer beliebigen Form stets geordnet werden. Sind nun

$$(8)\qquad \begin{aligned} E(v_1, \cdots v_m) &= U_1\eta^{(1)} + U_2\eta^{(2)} + \cdots\cdots + U_\lambda\eta^{(\lambda)},\\ F(v_1, \cdots v_m) &= V_1\zeta^{(1)} + V_2\zeta^{(2)} + \cdots + V_\mu\zeta^{(\mu)} \cdot \end{aligned}$$

zwei so geordnete Formen, in denen also U_1 und V_1 die Glieder höchster Ordnung sind, so besitzt in ihrem Produkte:

$$(8a)\qquad EF = U_1 V_1 \eta^{(1)}\zeta^{(1)} + \cdots + U_i V_k \eta^{(i)}\zeta^{(k)} + \cdots$$

das erste Glied $U_1 V_1$ ebenfalls die höchste Ordnung, denn jeder Quotient

$$\frac{U_i V_k}{U_1 V_1} = \left(\frac{U_i}{U_1}\right)\left(\frac{V_k}{V_1}\right)$$

ist von negativer Ordnung, weil dasselbe für die beiden Faktoren $\frac{U_i}{U_1}$ und $\frac{V_k}{V_1}$ der Fall ist. Hieraus folgt, daß sich dieses Anfangsglied $U_1 V_1 \eta^{(1)}\zeta^{(1)}$ für unbestimmte $v_1, \ldots v_m$ nicht fortheben kann, weil keines der folgenden Glieder $U_i V_k \eta^{(i)}\zeta^{(k)}$ dasselbe Exponentensystem besitzt.

Es mögen nun die beiden Formen $E(v_1, \ldots v_m)$ und $F(v_1, \ldots v_m)$ bzw. die Teiler $\mathfrak{E}$ und $\mathfrak{F}$ enthalten. Ich will dann den schon a. S. 313 unten angekündigten Beweis führen, daß der Teiler ihres Produktes

$$(9)\qquad E(v_1 \ldots v_m)\, F(v_1 \ldots v_m) = \sum_{i=1}^{\lambda}\sum_{k=1}^{\mu} U_i V_k \eta^{(i)}\zeta^{(k)}$$

genau gleich $\mathfrak{E}\mathfrak{F}$ ist. Da jedes Produkt $\eta^{(i)}\zeta^{(k)}$ durch $\mathfrak{E}\mathfrak{F}$ teilbar ist, so sieht man ohne weiteres, daß alle in (9) auftretenden Glieder des Produktes EF mindestens den Divisor $\mathfrak{E}\mathfrak{F}$ enthalten müssen. Zieht man dort aber alle Glieder in eines zusammen, für welche die zugehörigen Produkte $U_i V_k$ gleich sind, so könnte die so sich ergebende Form sehr wohl für unbestimmte v_i ein Vielfaches von $\mathfrak{E}\mathfrak{F}$ als gemeinsamen Teiler aller Koeffizienten enthalten. Zum Beweise des Fundamentalsatzes genügt es nun, zu zeigen, daß die Summe auf der rechten Seite von (9) für unbestimmte $v_1, \ldots v_m$ einen beliebig gegebenen Primteiler $\mathfrak{p}$ genau so oft enthält, als das Divisorenprodukt $\mathfrak{E}\mathfrak{F}$.

Es seien nun $\mathfrak{E}$ und $\mathfrak{F}$ bzw. durch $\mathfrak{p}^e$ und $\mathfrak{p}^f$, also $\mathfrak{E}\mathfrak{F}$ durch $\mathfrak{p}^{e+f}$ genau teilbar. Betrachtet man dann die Formen E und F in (8) bzw. modulo $\mathfrak{p}^{e+1}$ und $\mathfrak{p}^{f+1}$ und läßt in jeder von beiden von dem ersten Gliede anfangend alle diejenigen Glieder $U_1\eta^{(1)}, \ldots V_1\zeta^{(1)}, \ldots$ fort, deren Koeffizienten durch $\mathfrak{p}^{e+1}$ bzw. $\mathfrak{p}^{f+1}$ teilbar sind, so ergeben sich die beiden Kongruenzen:

$$(10)\qquad \begin{aligned} E &\equiv U_r\eta^{(r)} + U_{r+1}\eta^{(r+1)} + \cdots \pmod{\mathfrak{p}^{e+1}}\\ F &\equiv V_s\zeta^{(s)} + V_{s+1}\,\zeta^{(s+1)} + \cdots \pmod{\mathfrak{p}^{f+1}}. \end{aligned}$$

Hier sind also U_r und V_s diejenigen Produkte, deren Koeffizienten $\eta^{(r)}$ und $\zeta^{(s)}$ genau durch $\mathfrak{p}^e$ bzw. $\mathfrak{p}^f$ teilbar sind, und in denen U_r und V_s von höherer Ordnung sind als alle folgenden Produkte.

Multipliziert man nun die beiden Kongruenzen (10) und beachtet, daß alle Produkte, in denen auch nur ein fortgelassenes Glied vorkommt, mindestens durch $\mathfrak{p}^{e+f+1}$ teilbar sind, so ergibt sich modulo $\mathfrak{p}^{e+f+1}$ die Kongruenz:

$$EF \equiv U_r V_s \eta^{(r)} \zeta^{(s)} + U_r V_{s+1} \eta^{(r)} \zeta^{(s+1)} + \cdots \pmod{\mathfrak{p}^{e+f+1}}.$$

Da aber hier das Anfangsglied $\eta^{(r)}\zeta^{(s)}$ genau durch $\mathfrak{p}^{e+f}$ teilbar ist, und da es sich außerdem nach dem soeben bewiesenen Satze (8a) nicht gegen ein folgendes Glied fortheben kann, so ist gezeigt, daß das Formenprodukt EF diesen Primteiler $\mathfrak{p}$, also auch jeden anderen, genau in der gleichen Potenz enthält, wie das Divisorenprodukt $\mathfrak{E}\mathfrak{F}$; unser Satz ist also vollständig bewiesen.

Die für die Divisoren gegebenen Definitionen können nun ohne weiteres auf die ihnen gleichen Formen übertragen werden. Speziell nenne ich eine Form primitiv, wenn ihr Teiler gleich Eins ist, sie heißt eine Primform, wenn ihr Teiler ein Primdivisor ist; unter einer ganzen Form verstehe ich eine solche, deren Teiler ein ganzer Divisor ist, auch wenn sie als Funktion der Unbestimmten $v_1, \ldots v_m$ betrachtet nicht ganz sein sollte. Eine Form heißt durch eine andere teilbar, wenn der Divisor der ersten ein Vielfaches des Divisors der zweiten ist. Endlich ist jede ganze Form gleich dem Produkte einer endlichen Anzahl von Primformen, und diese Zerlegung ist eine eindeutige.

§ 4. Die Darstellung aller Divisoren durch zweigliedrige Formen.

Die Primformen konnten wir nun in besonders einfacher Weise, nämlich als zweigliedrige Formen darstellen. Ist nämlich p eine beliebige Primzahl, $\mathfrak{p}$ ein Primteiler von p, und π eine zu $\mathfrak{p}$ gehörige Primzahl, welche keinen der anderen Primteiler $\mathfrak{p}'$ von p enthält, so ist ja

(1) $$\mathfrak{p} = (p, \pi) = p + u\pi.$$

Ist speziell γ eine für $\mathfrak{p}$ reguläre algebraische Zahl, so konnten wir nach dem Satze (12b) a. S. 303 $\pi = \mathfrak{F}^{(0)}(\gamma)$, also

(1a) $$\mathfrak{p} = (p, \mathfrak{F}^{(0)}(\gamma)) = p + u\mathfrak{F}^{(0)}(\gamma)$$

setzen. Endlich läßt sich nach dem Theoreme (4) a. S. 312 auch jede positive Primteilerpotenz als zweigliedrige Form darstellen, denn aus (1) folgt ja:

(1b) $$\mathfrak{p}^r = (p^r, \pi^r) = p^r + u\pi^r.$$

Nach dem am Schlusse des vorigen Paragraphen bewiesenen allgemeinen Satze kann somit jeder ganze Divisor folgendermaßen dargestellt werden:

(2) $$\mathfrak{D} = \prod_{(\mathfrak{p})} \mathfrak{p}_i^{r_i} = \prod \left(p_i^{r_i}, \pi_i^{r_i}\right) = \prod \left(p_i^{r_i} + u_i \pi_i^{r_i}\right)$$

wo p_i jedesmal die zu dem betreffenden Primteiler $\mathfrak{p}_i$ gehörige reelle Primzahl bedeutet.

Ich zeigte soeben, daß sich alle Primteilerpotenzen $\mathfrak{p}^r$ als die größten gemeinsamen Teiler von nur zwei Zahlen des Körpers oder auch als zweigliedrige Linearformen darstellen lassen. Man wird dadurch zu dem Wunsche veranlaßt, zu untersuchen, ob nicht vielleicht alle ganzen und gebrochenen Teiler $\mathfrak{D}$ in der einfachen Form:

(3) $$\mathfrak{D} = (\alpha, \beta) = \alpha + \beta u$$

als größte gemeinsame Teiler von nur zwei Zahlen des Körpers oder als zweigliedrige Linearformen dargestellt werden können. Dies ist nun in der Tat der Fall; die Richtigkeit dieser Behauptung ergibt sich sofort aus dem folgenden Fundamentaltheoreme, welches mit voller Deutlichkeit erkennen läßt, daß die algebraischen Primteiler eines Körpers $K(\alpha)$ zu den Zahlen dieses Körpers in genau derselben Beziehung stehen, wie die reellen Primzahlen zu den rationalen Zahlen des Körpers $K(1)$:

> Die Primteiler eines Körpers $K(\alpha)$ sind in der Weise unabhängig voneinander, daß man stets eine Zahl dieser Körpers finden kann, welche für den Bereich von beliebig gewählten Primteilern
>
> (4) $$\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots \mathfrak{s}$$
>
> beliebig vorgegebene Entwicklungen bis zu Gliedern beliebig hoher Ordnung hat, während sie sich für den Bereich aller übrigen Primteiler regulär verhält.

Ich kann diesen wichtigen und höchst allgemeinen Satz leicht auf den folgenden speziellen Fall desselben reduzieren, welcher seinerseits wieder eine unmittelbare Folge aus dem auf S. 280 Mitte bewiesenen Theoreme ist.

> (4a) Es seien $p, q, r, \ldots s$ beliebige rationale Primzahlen, und M eine beliebig groß gegebene positive Zahl. Dann kann man stets eine algebraische Zahl T finden, deren n konjugierte Wurzeln für den Bereich von p modulo p^M beliebig vorgegebene Werte haben, welche ferner durch $(qr \ldots s)^M$ teilbar ist, und sich sonst überall regulär verhält.

Dieser Satz ist leicht zu beweisen: Ich zeigte auf S. 280 Mitte, das man eine algebraische Zahl T_0 finden kann, deren n konjugierte Entwicklungen für den Bereich von p bis zu Gliedern beliebig hoher Ordnung beliebig vorgegebene Werte haben, welche also der ersten der für T aufgestellten Forderung genügt. Die dort in (2a) gefundene Zahl

$$u_1^{(k)}\gamma^{(1)}+u_2^{(k)}\gamma^{(2)}+\cdots+u_n^{(k)}\gamma^{(n)}$$

verhält sich außerdem an allen nicht zu p gehörigen Stellen regulär, da die Zahlen $\gamma^{(i)}$ algebraisch ganz sind, und die rationalen Zahlen $u_i^{(k)}$ höchstens den Nenner p besitzen. Soll diese Zahl nun außerdem durch $(qr\ldots s)^M$ teilbar werden, so bestimme man, was ja stets möglich ist, eine ganze reelle rationale Zahl P_0 so, daß

$$P_0(qr\ldots s)^M\equiv 1 \quad (\text{und } p^M)$$

ist, daß also das links stehende Produkt für jede der Potenzen $q^M, \ldots s^M$ als Modul kongruent Null, aber modulo p^M kongruent Eins ist. Dann genügt die algebraische Zahl

$$\mathsf{T}=P_0(qr\ldots s)^M\mathsf{T}_0 \tag{5}$$

offenbar allen Anforderungen des Satzes (4a).

Um nun den allgemeinen Satz (4) zu beweisen nehme ich erstens an, die dort angegebenen Primteiler $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \ldots \mathfrak{s}$ gehören zu den reellen Primzahlen $p, q, r, \ldots s$, wobei aber nicht ausgeschlossen sein soll, daß auch mehrere verschiedene Primteiler $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ zu derselben reellen Primzahl p gehören. Zweitens möge für den Bereich aller dieser Primteiler die Entwicklung höchstens bis zu den Gliedern M^{ter} Ordnung vorgeschrieben sein; für diejenigen unter den Primteilern $\mathfrak{p}, \mathfrak{q}, \ldots$, für welche die Entwicklung nur bis zu Gliedern niedrigerer Ordnung gegeben sein sollte, mögen die fehlenden Glieder noch beliebig bestimmt werden, und ebenso denke ich mir für die zu den Primzahlen $p, q, r, \ldots s$ gehörigen Primteiler, welche nicht unter den Divisoren $\mathfrak{p}, \mathfrak{q}, \ldots$ vorkommen, für welche also keine Entwicklung vorgeschrieben ist, irgend eine aber reguläre Entwicklung bis zu den Gliedern M^{ter} Ordnung gegeben.

Ich wähle nun eine algebraische Zahl T in dem Körper $K(\alpha)$ so aus, daß sie erstens für alle zu p gehörigen Primteiler die vorgeschriebenen Entwicklungen bis zu den Gliedern M^{ter} Ordnung hat, daß sie zweitens durch das Produkt $(qr\ldots s)^M$ teilbar wird, und daß sie drittens für den Bereich aller übrigen Primteiler regulär ist, dies ist nach dem Hilfssatze (4a) stets möglich. Ebenso möge K eine Zahl sein, welche zu der zweiten reellen Primzahl q und dem Produkt

$(pr \ldots s)^M$ die gleiche Beziehung hat, usw. und die algebraische Zahl Σ soll entsprechend der letzten Primzahl s zugeordnet sein.

Dann erkennt man ohne weiteres, daß die aus ihnen zusammengesetzte Zahl:

(6) $$\beta = \mathsf{T} + \mathsf{K} + \cdots + \Sigma$$

allen Anforderungen unseres Satzes genügt; ist nämlich $\mathfrak{p}$ irgend einer der Primteiler unserer Reihe, so ist ja

$$\beta \equiv \mathsf{T} \pmod{\mathfrak{p}^M}$$

und T besitzt die für den Bereich von $\mathfrak{p}$ vorgeschriebene Entwicklung bis zu den Gliedern M^{ter} Ordnung.

Im nächsten Abschnitte werde ich einige wichtige Anwendungen dieses Satzes geben. Hier will ich ihn nur benutzen, um mit seiner Hilfe die am Anfang dieses Paragraphen aufgestellte Behauptung und zwar in der folgenden wesentlich schärferen Form zu beweisen:

Jeder ganze oder gebrochene Divisor $\mathfrak{D}$ des Körpers $K(\alpha)$ ist stets in der Form:

(7) $$\mathfrak{D} = (\beta, \gamma) = \beta + u\gamma,$$

d. h. als größter gemeinsamer Teiler von nur zwei algebraischen durch $\mathfrak{D}$ teilbaren Zahlen darstellbar, und zwar kann die eine von ihnen unter den Vielfachen von $\mathfrak{D}$ ganz beliebig ausgewählt werden.

In der Tat ist

(8) $$\beta = \mathfrak{D}\mathfrak{G}$$

eine beliebige durch $\mathfrak{D}$ teilbare Zahl, also $\mathfrak{G}$ ein ganzer Divisor, so braucht ja

(8a) $$\gamma = \mathfrak{D}\mathfrak{H}$$

unter den Vielfachen von $\mathfrak{D}$ nur so ausgewählt zu werden, daß der ganze Divisor $\mathfrak{H}$ zu $\mathfrak{G}$ teilerfremd ist; denn dann ist ja

(8b) $$(\beta, \gamma) = \mathfrak{D}(\mathfrak{G}, \mathfrak{H}) = \mathfrak{D}.$$

Dieser Forderung kann aber nach dem soeben bewiesenen Satze stets genügt werden. Ist nämlich $\mathfrak{p}$ irgend ein Primteiler des ganzen Divisors $\mathfrak{G}$, welcher in $\mathfrak{D}$ und $\mathfrak{G}$ bzw. d und g Male enthalten ist, so ist die algebraische Zahl γ nur so zu wählen, daß sie genau durch $\mathfrak{p}^d$ teilbar ist. Da nun der ganze Divisor $\mathfrak{G}$ nur eine endliche Anzahl von Primteilern enthält, so ergeben sich für die zu bestimmende Zahl γ auch nur eine endliche Anzahl von solchen Bedingungen, denen nach dem erwähnten Satze stets genügt werden kann; unsere Behauptung ist also vollständig bewiesen.

§ 5. Untersuchung der Zahlen eines Ideales für einen Divisor dieses Ideales als Modul. Der Fermatsche Satz für ganze Divisoren.

Ich benutze jetzt den im vorigen Paragraphen bewiesenen Satz von der Unabhängigkeit der Primteiler eines Körpers, um die Multipla eines ganzen oder gebrochenen Divisors $\mathfrak{D}$ oder die Zahlen eines Ideales $\mathfrak{J}(\mathfrak{D})$ genauer auf ihre Teilbarkeit zu untersuchen. Die hier gefundenen Resultate sollen dann speziell auf die Vielfachen des Divisors $\mathfrak{D} = 1$, d. h. auf den Bereich der ganzen algebraischen Zahlen angewendet werden.

Es sei also $\mathfrak{D}$ irgend ein Divisor des Körpers $K(\alpha)$ und

$$(1) \qquad \mathfrak{M} = \mathfrak{D}\mathfrak{G}$$

ein beliebiges Multiplum von $\mathfrak{D}$, so daß $\mathfrak{G}$ ein ganzer Divisor ist; dann kann und soll $\mathfrak{M}$ als ein Divisor des zu $\mathfrak{D}$ gehörigen Ideales $\mathfrak{J}(\mathfrak{D})$ bezeichnet werden. Ich will nun die Zahlen des Bereiches $\mathfrak{J}(\mathfrak{D})$ auf ihre Teilbarkeit durch $\mathfrak{M}$ untersuchen und insbesondere ein vollständiges Restsystem für die Multipla von $\mathfrak{D}$ modulo $\mathfrak{M}$ bestimmen. Es sei nun $\mathfrak{p}$ irgend ein Primteiler von der Ordnung e und vom Grade f; p sei die zugehörige reelle Primzahl, und es mögen $\mathfrak{p}^d$ und $\mathfrak{p}^m$ die in $\mathfrak{D}$ und $\mathfrak{M}$ enthaltenen Potenzen von $\mathfrak{p}$ sein. Da $\mathfrak{M}$ ein Vielfaches von $\mathfrak{D}$ ist, so muß $m \geqq d$ sein.

Jede durch $\mathfrak{D}$, also auch durch $\mathfrak{p}^d$ teilbare Zahl von $K(\alpha)$ ist dann für den Bereich von $\mathfrak{p}$ gleich:

$$(2) \qquad A_d \pi^d + A_{d+1} \pi^{d+1} + \cdots,$$

wo π eine zu $\mathfrak{p}$ gehörige Primzahl ist, und jeder der Koeffizienten

$$(2\text{a}) \qquad A_i = \overset{(i)}{a}_0 + \overset{(i)}{a}_1 \eta + \cdots + \overset{(i)}{a}_{f-1} \eta^{f-1}$$

eine modulo p reduzierte ganze Zahl des zu $\mathfrak{p}$ gehörigen Koeffizientenkörpers bedeutet. Jeder dieser Koeffizienten kann also $p^f = n(\mathfrak{p})$ verschiedene Werte annehmen. Umgekehrt kann man nach dem im vorigen Paragraphen bewiesenen Satze auch stets eine durch $\mathfrak{D}$ teilbare algebraische Zahl des Körpers finden, welche bis zu Gliedern einer beliebig vorgeschriebenen Ordnung eine beliebig angenommene Entwicklung (2) für den Bereich von $\mathfrak{p}$ besitzt.

Jede Zahl des Bereiches $\mathfrak{J}(\mathfrak{D})$ ist nun modulo $\mathfrak{p}^m$ betrachtet einer und nur einer der $p^{f(m-d)}$ Zahlen:

$$(3) \qquad A_d \pi^d + A_{d+1} \pi^{d+1} + \cdots + A_{m-1} \pi^{m-1}$$

kongruent, welche man erhält, wenn man jedem der m Koeffizienten $A_d, A_{d+1}, \ldots A_{m-1}$ unabhängig von den übrigen seine p^f modulo p inkongruenten Werte beilegt, und man kann auch stets $p^{f(m-d)}$ Zahlen des Bereiches $\mathfrak{J}(\mathfrak{D})$ finden, welche modulo $\mathfrak{p}^m$ betrachtet gerade diesen

Zahlen kongruent sind; diese Zahlen bilden dann also ein vollständiges Restsystem für die Zahlen von $\mathfrak{J}(\mathfrak{D})$ in Beziehung auf den Divisor $\mathfrak{p}^m$, und ihre Anzahl $\mathfrak{A}(\mathfrak{p}^m)$ ist durch die Gleichung

(4) $$\mathfrak{A}(\mathfrak{p}^m) = p^{f(m-d)} = n\left(\frac{\mathfrak{p}^m}{\mathfrak{p}^d}\right)$$

bestimmt.

Es seien nun $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_r$ alle Primteiler, welche mindestens in einem der beiden Divisoren $\mathfrak{D}$ und $\mathfrak{M}$ wirklich vorkommen, $p_1, p_2, \ldots p_r$ die zu ihnen gehörigen reellen Primzahlen, und es mögen:

(5) $$\mathfrak{D} = \mathfrak{p}_1^{d_1}\mathfrak{p}_2^{d_2}\cdots\mathfrak{p}_r^{d_r}, \qquad \mathfrak{M} = \mathfrak{p}_1^{m_1}\mathfrak{p}_2^{m_2}\cdots\mathfrak{p}_r^{m_r}$$

die Zerlegungen von $\mathfrak{D}$ und $\mathfrak{M}$ sein. Dann ist allgemein die Anzahl aller modulo $\mathfrak{p}_i^{m_i}$ inkongruenten Zahlen des Bereiches $\mathfrak{J}(\mathfrak{D})$ gleich $n\left(\frac{\mathfrak{p}_i^{m_i}}{\mathfrak{p}_i^{d_i}}\right)$, und man kann nach dem im vorigen Paragraphen bewiesenen Satze (4) a. S. 317 stets eine durch $\mathfrak{D}$ teilbare Zahl finden, welche für jede der r Primzahlpotenzen $\mathfrak{p}_i^{m_i}$ als Modul einer der $n\left(\frac{\mathfrak{p}_i^{m_i}}{\mathfrak{p}_i^{d_i}}\right)$ Zahlen des vollständigen Restsystemes modulo $\mathfrak{p}_i^{m_i}$ kongruent ist. Die so sich ergebenden Zahlen des Bereiches $\mathfrak{J}(\mathfrak{D})$, deren Anzahl offenbar gleich $\mathfrak{A}(\mathfrak{p}_1^{m_1}) \ldots \mathfrak{A}(\mathfrak{p}_r^{m_r})$ ist, bilden dann ein vollständiges Restsystem für die Multipla von $\mathfrak{D}$ modulo $\mathfrak{M}$, denn sie sind erstens alle durch $\mathfrak{D}$ teilbar, zweitens sind sie modulo $\mathfrak{M}$ inkongruent, da ja je zwei unter ihnen mindestens für einen Divisor $\mathfrak{p}_i^{m_i}$ als Modul verschiedene Entwicklungen haben, und drittens ist jede durch $\mathfrak{D}$ teilbare Zahl β einer Zahl dieses Systemes modulo $\mathfrak{M}$ kongruent, denn es gibt unter jenen Zahlen eine einzige, welche zu β für jede der r Primzahlpotenzen $\mathfrak{p}_i^{m_i}$ also auch für ihr Produkt $\mathfrak{M}$ kongruent ist. Nach (4) ist also diese Anzahl der modulo $\mathfrak{M}$ inkongruenten Multipla von $\mathfrak{D}$ gleich:

(6) $$\mathfrak{A}(\mathfrak{p}_1^{m_1})\cdots\mathfrak{A}(\mathfrak{p}_r^{m_r}) = n\left(\frac{\mathfrak{p}_1^{m_1}\mathfrak{p}_2^{m_2}\cdots\mathfrak{p}_r^{m_r}}{\mathfrak{p}_1^{d_1}\mathfrak{p}_2^{d_2}\cdots\mathfrak{p}_r^{d_r}}\right) = n\left(\frac{\mathfrak{M}}{\mathfrak{D}}\right) = n(\mathfrak{G}).$$

Die Norm braucht hier nur über alle Primteiler des ganzen Divisors $\mathfrak{G}$, d. h. über diejenigen erstreckt zu werden, welche öfter in $\mathfrak{M}$ als in $\mathfrak{D}$ enthalten sind. Diese Anzahl ist somit allein von dem Quotienten $\frac{\mathfrak{M}}{\mathfrak{D}}$ abhängig, bleibt also ungeändert, wenn $\mathfrak{M}$ und $\mathfrak{D}$ beide mit demselben Divisor multipliziert werden. Dieses letzte Resultat kann auch leicht

direkt verifiziert werden, was dem Leser überlassen bleiben möge. Es ergibt sich also jetzt der Satz:

(7) Ist $\mathfrak{D}$ ein beliebiger ganzer oder gebrochener Divisor von $K(\alpha)$ und $\mathfrak{M} = \mathfrak{D}\mathfrak{G}$ irgend ein Vielfaches von $\mathfrak{D}$, ist also $\mathfrak{M}$ ein Divisor des zu $\mathfrak{D}$ gehörigen Ideales $\mathfrak{J}(\mathfrak{D})$, so ist die Anzahl aller modulo $\mathfrak{M}$ inkongruenten Multipla von $\mathfrak{D}$ stets gleich der Norm des Quotienten $\frac{\mathfrak{M}}{\mathfrak{D}} = \mathfrak{G}$.

Ist speziell $\mathfrak{D} = 1$, ist also der Bereich der Multipla von $\mathfrak{D}$ das Gebiet der ganzen algebraischen Zahlen, so muß $\mathfrak{M} = \mathfrak{G}\mathfrak{D} = \mathfrak{G}$ irgend ein ganzer Divisor sein. Dann ergibt sich also die Folgerung:

(7a) Ist $\mathfrak{M}$ irgend ein ganzer Divisor von $K(\alpha)$, so ist die Anzahl aller modulo $\mathfrak{M}$ inkongruenten ganzen algebraischen Zahlen gleich der Norm dieses Divisors.

Es sei wieder $\mathfrak{D}$ ein beliebiger Divisor, und

(8) $$\mathfrak{M} = \mathfrak{D}\mathfrak{G}$$

irgend ein anderer Divisor, welcher ein Vielfaches von $\mathfrak{D}$ ist, also ein Divisor des Ideals $\mathfrak{J}(\mathfrak{D})$. Jede algebraische Zahl

(8a) $$\beta = \mathfrak{D}\mathfrak{B},$$

welche dem Ideale $\mathfrak{J}(\mathfrak{D})$ angehört, hat dann mit $\mathfrak{M}$ den gemeinsamen Teiler $\mathfrak{D}$, weil:

(8b) $$(\mathfrak{M}, \beta) = \mathfrak{D}(\mathfrak{G}, \mathfrak{B})$$

ist, und $\mathfrak{G}$ und $\mathfrak{B}$ ganze Divisoren sind. Dann und nur dann ist $\mathfrak{D}$ der größte gemeinsame Teiler von $\mathfrak{M}$ und β, wenn $\mathfrak{B}$ zu $\mathfrak{G}$ teilerfremd ist, wenn also β jeden in $\mathfrak{G}$ enthaltenen Primteiler genau so oft enthält als er in $\mathfrak{D}$ vorkommt.

Ich stelle mir jetzt die Aufgabe, ein vollständiges System aller modulo $\mathfrak{M}$ inkongruenten Zahlen des Bereiches $\mathfrak{J}(\mathfrak{D})$ zu bestimmen, welche mit $\mathfrak{M}$ den größten gemeinsamen Teiler $\mathfrak{D}$ besitzen. Ein solches System finde ich nach der soeben gemachten Bemerkung, wenn ich aus dem vollständigen Restsysteme modulo $\mathfrak{M}$ alle diejenigen Zahlen fortlasse, welche auch nur einen der in $\mathfrak{G}$ enthaltenen Primfaktoren öfter enthalten als er in $\mathfrak{D}$ vorkommt.

Es sei nun β eine der $n(\mathfrak{G})$ modulo $\mathfrak{M}$ inkongruenten Multipla von $\mathfrak{D}$. Ist dann wieder $\mathfrak{p}$ einer der in $\mathfrak{G}$ enthaltenen Primteiler, welcher d Male in $\mathfrak{D}$ und m Male in $\mathfrak{M}$ enthalten ist, so besteht modulo $\mathfrak{p}^m$ eine Kongruenz von der Form:

(9) $$\beta \equiv A_d\pi^d + A_{d+1}\pi^{d+1} + \cdots + A_{m-1}\pi^{m-1} \pmod{\mathfrak{p}^m},$$

und β ist dann und nur dann genau durch $\mathfrak{p}^d$ teilbar, wenn $A_d \gtrless 0$ ist, während alle folgenden Koeffizienten ganz beliebig angenommen

werden können. Von den $p^{f(m-d)}$ modulo $\mathfrak{p}^m$ inkongruenten Zahlen (9) sind somit alle und nur die $p^{f(m-d-1)}$ Zahlen:

$$A_{d+1}\pi^{d+1} + \cdots + A_{m-1}\pi^{m-1}$$

fortzulassen, in denen $A_d = 0$ ist, und es bleiben:

$$(10) \qquad p^{f(m-d)}\left(1 - \frac{1}{p^f}\right) = n\left(\frac{\mathfrak{p}^m}{\mathfrak{p}^d}\right)\left(1 - \frac{1}{n(\mathfrak{p})}\right)$$

modulo $\mathfrak{p}^m$ inkongruente Zahlen übrig, welche genau durch $\mathfrak{p}^d$ teilbar sind.

Aus der ganzen Reihe der $n(\mathfrak{G})$ modulo $\mathfrak{M}$ inkongruenten Vielfachen von β sind also nur diejenigen beizubehalten, deren Entwicklungen für den Bereich aller in $\mathfrak{G} = \frac{\mathfrak{M}}{\mathfrak{D}}$ enthaltenen Primteiler $\mathfrak{p}$ mit der niedrigsten Potenz π^d der zugehörigen Primzahl beginnen. Es bleiben dann alle und nur die Zahlen übrig, welche für jede der Divisorenpotenzen $\mathfrak{p}^m$ als Modul je einer beliebigen unter den vorher charakterisierten Entwicklungen kongruent sind. Also ist die Gesamtanzahl $\varphi(\mathfrak{M}, \mathfrak{D})$ aller Vielfachen von $\mathfrak{D}$, welche mit $\mathfrak{M}$ den größten gemeinsamen Teiler $\mathfrak{D}$ haben, durch die folgende Gleichung bestimmt:

$$(11) \quad \varphi(\mathfrak{M}, \mathfrak{D}) = \prod_{\mathfrak{p} \mid \frac{\mathfrak{M}}{\mathfrak{D}}} n\left(\frac{\mathfrak{p}^m}{\mathfrak{p}^d}\right)\left(1 - \frac{1}{n(\mathfrak{p})}\right) = n\left(\frac{\mathfrak{M}}{\mathfrak{D}}\right) \cdot \prod_{\mathfrak{p} \mid \frac{\mathfrak{M}}{\mathfrak{D}}}\left(1 - \frac{1}{n(\mathfrak{p})}\right),$$

wo sich das Produkt auf alle verschiedenen Primteiler von $\frac{\mathfrak{M}}{\mathfrak{D}} = \mathfrak{G}$ bezieht. Auch hier ist diese Anzahl allein von dem Quotienten $\frac{\mathfrak{M}}{\mathfrak{D}} = \mathfrak{G}$ abhängig.

Der wichtigste spezielle Fall ist wieder der, daß $\mathfrak{D} = 1$, daß also $\mathfrak{M} = \mathfrak{G}$ ein beliebiger ganzer Divisor ist. Alsdann gibt $\varphi(\mathfrak{G}, 1) = \varphi(\mathfrak{G})$ die Anzahl aller modulo $\mathfrak{G}$ inkongruenten ganzen algebraischen Zahlen, welche zu dem ganzen Divisor $\mathfrak{G}$ teilerfremd sind. Diese Anzahl ist mithin die genaue Verallgemeinerung der Eulerschen arithmetischen Funktion $\varphi(m)$. Wir erhalten also den Satz:

Die Anzahl aller modulo $\mathfrak{G}$ inkongruenten und zu $\mathfrak{G}$ teilerfremden ganzen Zahlen des Körpers $K(\alpha)$ ist gleich

$$(11\text{a}) \qquad \varphi(\mathfrak{G}) = n(\mathfrak{G}) \prod_{\mathfrak{p} \mid \mathfrak{G}} \left(1 - \frac{1}{n(\mathfrak{p})}\right),$$

wenn $\mathfrak{G}$ ein beliebiger ganzer Divisor ist.

Dieser Satz ergibt eine einfache Verallgemeinerung der Darstellung der arithmetischen Funktion

$$(11\text{b}) \qquad \varphi(g) = g \prod_{p \mid g} \left(1 - \frac{1}{p}\right),$$

wenn g eine ganze rationale Zahl ist, und sie besitzt genau dieselben Eigenschaften wie jene. Ist speziell $\mathfrak{G} = \mathfrak{p}^g$ die Potenz eines einzigen Primteilers, so ist

(12) $$\varphi(\mathfrak{p}^g) = n(\mathfrak{p})^g - n(\mathfrak{p})^{g-1}.$$

Ist ferner $\mathfrak{G} = \mathfrak{A} \cdot \mathfrak{B}$ das Produkt von zwei teilerfremden ganzen Divisoren, so folgt ebenfalls aus der allgemeinen Darstellung (11a) von $\varphi(\mathfrak{G})$, daß stets:

(12a) $$\varphi(\mathfrak{A}\mathfrak{B}) = \varphi(\mathfrak{A})\,\varphi(\mathfrak{B})$$

ist. Eine unmittelbare Konsequenz dieser beiden Sätze ist das folgende allgemeine Theorem:

Ist $\mathfrak{G}$ ein beliebiger ganzer Divisor, so besteht immer die Gleichung:

(13) $$\sum_{\mathfrak{D}\mid\mathfrak{G}} \varphi(\mathfrak{D}) = n(\mathfrak{G}),$$

wenn $\mathfrak{D}$ alle ganzen Divisoren von $\mathfrak{G}$ durchläuft.

Ist nämlich zunächst $\mathfrak{G} = \mathfrak{p}^g$ eine Primdivisorpotenz, so ist die obige Gleichung richtig, denn aus (12) folgt ja:

(14) $$P = \sum_{\mathfrak{D}\mid\mathfrak{p}^g} \varphi(\mathfrak{D}) = \sum_{i=0}^{g} \varphi(\mathfrak{p}^i) = 1 + \sum_{i=1}^{g} (n(\mathfrak{p}^i) - n(\mathfrak{p}^{i-1})) = n(\mathfrak{p}^g),$$

w. z. b. w.

Um denselben Satz für einen beliebigen zusammengesetzten Divisor:

(15) $$\mathfrak{G} = \mathfrak{p}^g \mathfrak{q}^h \cdots \mathfrak{r}^k$$

zu beweisen, bilde ich das folgende Produkt:

(16) $$PQ \cdots R = (\varphi(1) + \varphi(\mathfrak{p}) + \cdots + \varphi(\mathfrak{p}^g))\,(\varphi(1) + \varphi(\mathfrak{q}) + \cdots + \varphi(\mathfrak{q}^h)) \cdots (\varphi(1) + \varphi(\mathfrak{r}) + \cdots + \varphi(\mathfrak{r}^k)).$$

Die Faktoren $P, Q, \ldots R$ der rechten Seite sind nach (14) bzw. gleich $n(\mathfrak{p}^g), n(\mathfrak{q}^h), \ldots n(\mathfrak{r}^k)$, der Wert ihres Produktes ist also gleich $n(\mathfrak{G})$. Multipliziert man dagegen die rechte Seite aus und beachtet, daß dann jedes der Produkte:

$$\varphi(\mathfrak{p}^{g_0})\,\varphi(\mathfrak{q}^{h_0}) \ldots \varphi(\mathfrak{r}^{k_0}) \qquad \begin{pmatrix} g_0 = 0, 1, \cdots g \\ h_0 = 0, 1, \cdots h \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ k_0 = 0, 1, \cdots k \end{pmatrix}$$

nach dem Satze (12a) in der Form

$$\varphi(\mathfrak{p}^{g_0}\mathfrak{q}^{h_0} \cdots \mathfrak{r}^{k_0}) = \varphi(\mathfrak{D})$$

geschrieben werden kann, wenn $\mathfrak{D}$ alle Teiler von $\mathfrak{G}$ durchläuft, so ist jenes Produkt auch gleich $\sum_{\mathfrak{D}\mid\mathfrak{G}} \varphi(\mathfrak{D})$. Damit ist die Richtigkeit der Gleichung (13) bewiesen.

Zum Abschluß dieser Untersuchungen beweise ich noch den sog. **Fermatschen Satz** für die ganzen Zahlen von $K(\alpha)$ in bezug auf einen beliebigen ganzen Divisor $\mathfrak{G}$. Es sei

(17) $$\beta_1, \beta_2, \dots \beta_{\varphi(\mathfrak{G})}$$

ein vollständiges Restsystem in bezug auf den Divisor $\mathfrak{G}$, und β eine beliebige aber zu $\mathfrak{G}$ teilerfremde ganze Zahl. Dann leuchtet ein, daß die $\varphi(\mathfrak{G})$ Produkte:

(17a) $$\beta\beta_1, \beta\beta_2, \dots \beta\beta_{\varphi(\mathfrak{G})}$$

sämtlich modulo $\mathfrak{G}$ inkongruent sind, und ferner, daß dieselben wieder relative Primzahlen zu $\mathfrak{G}$ sind; es wird daher jedes dieser Produkte einem und nur einem Gliede der Reihe (17) kongruent sein. Das Produkt aller Zahlen (17a) ist also dem der Zahlen (17) modulo $\mathfrak{G}$ kongruent, d. h. es ist:

$$\beta^{\varphi(\mathfrak{G})}(\beta_1 \cdots \beta_{\varphi(\mathfrak{G})}) \equiv (\beta_1 \cdots \beta_{\varphi(\mathfrak{G})}) \pmod{\mathfrak{G}},$$

und da das links und rechts stehende Produkt zu $\mathfrak{G}$ teilerfremd ist, so ergibt sich die Kongruenz:

(18) $$\beta^{\varphi(\mathfrak{G})} \equiv 1 \pmod{\mathfrak{G}},$$

welche den verallgemeinerten Fermatschen Satz im Gebiete der ganzen algebraischen Zahlen ausspricht.

Zwölftes Kapitel.

Die Darstellung der algebraischen Zahlen ihrer Größe nach und für den Bereich einer Primzahl.

§ 1. Untersuchung der p-adischen algebraischen Zahlen eines Körpers in bezug auf ihre Größe.

Im § 5 des zweiten Kapitels zeigte ich bereits, daß man jede rationale Zahl B so in eine konvergente nach ganzen Potenzen von p fortschreitende Reihe:

$$B = \sum b_i p^i$$

mit gewöhnlichen rationalen Zahlkoeffizienten entwickeln kann, daß sie sowohl ihrer Größe nach, als auch für den Bereich von p gegen den Grenzwert B konvergiert, daß sich also ihre Näherungswerte

$$B^{(k)} = b_0 + b_1 p + \cdots + b_k p^k \qquad (k = 0, 1, \ldots)$$

mit wachsendem k der Größe nach und für den Bereich von p um beliebig wenig von B unterscheiden. Dann ergab sich a. S. 46, daß eine beliebige rationale Gleichung:

$$\varphi(x, y, \cdots z) = 0$$

mit rationalen Zahlkoeffizienten dann und nur dann durch die p-adischen Entwicklungen der rationalen Zahlen

$$x = B, \;\; y = C, \;\cdots\; z = D$$

ihrer Größe nach mit jeder vorgegebenen Genauigkeit erfüllt wird, wenn sie für den Bereich von p besteht und umgekehrt.

Ebenso zeigte ich im § 8 des vierten Kapitels, daß auch die Wurzeln einer algebraischen Gleichung $f(x) = 0$ sowohl ihrer Größe nach, als auch für den Bereich von p durch rationale p-adische Zahlen dargestellt werden können, aber nur unter der Voraussetzung, daß diese Gleichung wenigstens eine rationale p-adische Wurzel

besitzt. Als Beispiel betrachtete ich a. S. 91 (4) die Kreisteilungsgleichung des $(p-1)^{\text{ten}}$ Grades:

$$x^{p-1} - 1 = 0,$$

welche ja für den Bereich von p genau $p-1$ rationale p-adische Wurzeln

$$1, \omega, \omega^2, \cdots \omega^{p-2}$$

besitzt, und zeigte, daß sie alle stets so in konvergente p-adische Reihen entwickelt werden können, daß jede zwischen ihnen der Größe nach bestehende rationale Gleichung mit rationalen Koeffizienten auch für den Bereich von p erfüllt ist, und umgekehrt.

Ich will nun den schon am Schlusse des vierten Kapitels in Aussicht gestellten Fundamentalsatz beweisen, daß man überhaupt alle algebraischen Zahlen für den Bereich einer beliebigen Primzahl p so in konvergente p-adische Reihen entwickeln kann, daß jede zwischen ihnen der Größe nach bestehende rationale Gleichung mit rationalen Koeffizienten auch für den Bereich von p erfüllt ist und umgekehrt. Ich weise dies zuerst für die algebraischen Zahlen eines und desselben Körpers nach.

Es sei $K(\alpha)$ ein beliebiger durch eine algebraische Zahl α konstituierter Körper n^{ter} Ordnung, und

$$F(x) = x^n + b_1 x^{n-1} + \cdots + b_n = 0 \tag{1}$$

die ihn definierende Grundgleichung. Ist dann p eine beliebige reelle Primzahl, $\mathfrak{p}$ einer ihrer Primteiler innerhalb $K(\alpha)$, dessen Ordnung gleich e und dessen Grad gleich f ist, und bedeutet ferner

$$1, \varepsilon, \ldots \varepsilon^{f-1}, \pi, \pi\varepsilon, \ldots \pi\varepsilon^{f-1}, \ldots \pi^{e-1}, \pi^{e-1}\varepsilon, \ldots \pi^{e-1}\varepsilon^{f-1} \tag{2}$$

ein Fundamentalsystem jenes Körpers für den Bereich von $\mathfrak{p}$, so ist jede Zahl von $K(\alpha)$, speziell also auch die Grundzahl α selbst für den Bereich von $\mathfrak{p}$ auf eine einzige Art in der Form:

$$\alpha = \sum_{i=0}^{f-1} \sum_{k=0}^{e-1} c_{ik} \varepsilon^i \pi^k \quad (\mathfrak{p}) \tag{3}$$

darstellbar, wo die c_{ik} für den Bereich von p eindeutig bestimmte rationale p-adische Zahlen bedeuten.

Ich bezeichne nun durch denselben Buchstaben α der Größe nach eine beliebige aber ein für alle Male fest bestimmte unter den n reellen oder komplexen Wurzeln derselben Grundgleichung (1) und will nun die ef p-adischen Reihen c_{ik} so bestimmen, daß sie auch der Größe nach unbedingt konvergieren, und daß:

(4) $$\alpha = \sum_{i=0}^{f-1} \sum_{k=0}^{e-1} c_{ik} \varepsilon^i \pi^k$$

ist. Dieser Forderung kann stets und zwar auf mannigfache aber nur formal verschiedene Weisen genügt werden, denn ich hatte ja a. S. 44 Mitte gezeigt, daß man die Koeffizienten einer p-adischen Reihe als komplexe Zahlen mit rationalen modulo p ganzen Koeffizienten stets so bestimmen kann, daß diese Reihe ihrer Größe nach gegen eine beliebig gegebene reelle oder komplexe Zahl, und für den Bereich von p gegen eine willkürlich angenommene p-adische Zahl konvergiert.

Am einfachsten können wir hier unser Ziel erreichen, wenn wir über die ef Koeffizienten $c_{00}, c_{01}, c_{10}, \ldots c_{f-1, e-1}$ so verfügen, daß der erste c_{00} der Größe nach gleich der Gleichungswurzel α wird, während die $ef - 1$ übrigen ihrer Größe nach alle gegen Null konvergieren. Für den Bereich von p dagegen sollen die ef Zahlen c_{ik} die durch die Gleichung (3) eindeutig bestimmten Werte haben. Sind die Koeffizienten c_{ik} in dieser Weise bestimmt, so ist sowohl der Größe nach, als auch für den Bereich von p

(5) $$\sum_i \sum_k c_{ik} \varepsilon^i \pi^k = \alpha,$$

wenn α eine beliebige unter den n Wurzeln bedeutet, welche die Grundgleichung der Größe nach bzw. für den Bereich von p besitzt. Die so bestimmte Reihe soll die p-adische Darstellung der algebraischen Zahl α genannt werden. Es ist klar, daß die Größenbestimmung für die ef Koeffizienten c_{ik} mannigfach variiert werden kann; jedesmal aber erhält man eine p-adische Darstellung der Zahl α, welche sowohl der Größe nach als auch für den Bereich von p mit der soeben angegebenen übereinstimmt.

Substituiert man nun in (5) für die Koeffizienten c_{ik} die p-adischen Reihen und ordnet dann die Reihe nach Potenzen von p und von π, so ergibt sich für α eine Darstellung:

(5a) $$\alpha = \sum_{k=0}^{e-1} \sum_{l=0}^{\infty} A_{kl}(\varepsilon, i)\, \pi^k p^l,$$

in welcher die Koeffizienten $A_{kl}(\varepsilon, i)$ modulo p ganze Zahlen des Koeffizientenkörpers $K(\varepsilon)$ mit reellen oder komplexen Koeffizienten sind. So ergibt sich also zunächst eine sowohl der Größe nach als auch für den Bereich von p unbedingt konvergente Reihe, welche nach ganzen Potenzen der Primzahl p und der algebraischen Zahl $\pi \sim p^{\frac{1}{e}}$

fortschreitet. Es ist nun leicht aus dieser Reihe für α eine andere herzuleiten, welche nach ganzen Potenzen von π allein fortschreitet.

Genügt nämlich zunächst π einer reinen Gleichung e^{ten} Grades

$$(6)\qquad \pi^e - p\,C_e(\varepsilon) = 0,$$

in welcher $C_e(\varepsilon)$ eine gewöhnliche ganze Zahl von $K(\varepsilon)$, aber eine Einheit modulo p ist, so folgt ja aus ihr

$$(6\text{a})\qquad p^l = \frac{\pi^{le}}{(C_e(\varepsilon))^l} \qquad (l = 0, 1, 2, \ldots),$$

und die Substitution dieser Werte in (5) liefert eine nach steigenden Potenzen von π allein geordnete Reihe:

$$(6\text{b})\qquad \alpha = \varepsilon_r \pi^r + \varepsilon_{r+1}\pi^{r+1} + \cdots$$

für α, in welcher die Koeffizienten ε_i nun gewöhnliche modulo p ganze Zahlen des Körpers $K(\varepsilon, i)$ bedeuten, und welche ebenfalls sowohl der Größe nach als auch für den Bereich von p gegen die vorher gewählten Wurzeln α der Grundgleichung konvergiert.

Genau dasselbe einfache Resultat ergibt sich auch in dem Falle, daß die Zahl π als e^{te} Wurzel aus p durch eine allgemeinere Eisensteinsche Gleichung:

$$(6\text{c})\qquad \pi^e - p(C_1(\varepsilon)\pi^{e-1} + C_2(\varepsilon)\pi^{e-2} + \cdots + C_e(\varepsilon)) = \pi^e - p\,\varphi(\varepsilon, \pi)$$

definiert ist, in welcher jetzt also $\varphi(\varepsilon, \pi)$ eine ganze rationale Funktion von ε und π mit gewöhnlichen ganzzahligen Koeffizienten bedeutet. Dies tritt nach dem a. S. 208 bewiesenen Satze nur in dem Ausnahmefall ein, daß e durch p teilbar ist. Hier ergibt sich durch Auflösung nach p

$$(6\text{d})\qquad p = \frac{\pi^e}{\varphi(\varepsilon, \pi)},$$

oder wenn $\Phi(\varepsilon, \pi)$ den zu $\varphi(\varepsilon, \pi)$ komplementären Faktor bedeutet, für welchen $\varphi(\varepsilon, \pi)\,\Phi(\varepsilon, \pi) = n(\varphi(\varepsilon, \pi)) = m$ ist,

$$(6\text{e})\qquad p = \frac{\pi^e \cdot \Phi(\varepsilon, \pi)}{m},$$

wo $\frac{\Phi(\varepsilon, \pi)}{m}$ eine ganze Funktion von ε und π mit gewöhnlichen rationalen aber modulo p ganzen Faktoren bedeutet, weil ja $\varphi(\varepsilon, \pi)$ eine algebraische, also $m = n(\varphi(\varepsilon, \pi))$ eine rationale Einheit modulo p bedeutet. Substituiert man nun diesen Wert von p in (5a) und ordnet wieder nach Potenzen von π, so erhält man auch hier für α die obige Darstellung (6b).

Ebenso läßt sich jede andere Zahl $\beta = \psi(\alpha)$ des Körpers $K(\alpha)$ in eine nach steigenden ganzen Potenzen von π fortschreitende Reihe

entwickeln, deren Koeffizienten modulo p ganze Zahlen des Körpers $K(\varepsilon, i)$ sind, und welche sowohl der Größe nach, als auch für den Bereich von p gegen $\psi(\alpha)$ konvergiert. In der Tat kann man ja β stets in der Form:

$$\beta = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}$$

mit gewöhnlichen rationalen Zahlkoeffizienten dargestellt voraussetzen, und die Substitution der Reihe (6b) für α liefert sofort die gesuchte Reihe für β.

Ist also $\alpha = \varepsilon_r \pi^r + \varepsilon_{r+1}\pi^{r+1} + \cdots$ die p-adische Darstellung einer Wurzel der Grundgleichung $f(x) = 0$, so können alle Zahlen β des Körpers $K(\alpha)$ in konvergente algebraische Potenzreihen

$$\beta = \sum_\lambda \bar{\varepsilon}_\lambda \pi^\lambda$$

so entwickelt werden, daß sie diese Zahlen sowohl der Größe nach als auch für den Bereich von $\mathfrak{p}$ darstellen.

Aus dem soeben bewiesenen Satze ziehe ich nun eine wichtige Folgerung: Es seien:

$$\beta = g(\alpha), \quad \gamma = h(\alpha), \cdots \delta = k(\alpha) \tag{7}$$

irgendwelche rationale Funktionen von α mit gewöhnlichen rationalen Zahlkoeffizienten, d. h. also beliebige algebraische Zahlen des durch α konstituierten Körpers $K(\alpha)$. Dann besteht zunächst der Satz:

Jede rationale Gleichung:

$$\varphi(\beta, \gamma, \cdots \delta) = 0 \tag{8}$$

mit rationalen Zahlkoeffizienten zwischen beliebig vielen Zahlen des Körpers $K(\alpha)$ bleibt richtig, wenn man sie als Gleichung für den Bereich von $\mathfrak{p}$ auffaßt, und umgekehrt folgt aus dem Bestehen einer solchen Gleichung:

$$\varphi(\beta, \gamma, \cdots \delta) = 0 \quad (\mathfrak{p}) \tag{8a}$$

für den Bereich von $\mathfrak{p}$, daß dieselbe Gleichung auch ihrer Größe nach erfüllt ist.

Besteht nämlich die Gleichung (8) ihrer Größe nach, und substituiert man in ihr für die Zahlen $\beta, \gamma, \ldots \delta$ ihre Ausdrücke (7) durch α, so geht ihre linke Seite in eine rationale Funktion von α mit gewöhnlichen rationalen Zahlkoeffizienten über, welche in ihrer reduzierten Form durch $\Phi(\alpha)$ bezeichnet werden möge. Wegen der Irreduktibilität der Grundgleichung (1) für α im Bereiche der rationalen Zahlen kann nun die Gleichung $\Phi(\alpha) = 0$ nur dann bestehen, wenn

die Funktion $\Phi(x)$ durch $F(x)$ teilbar ist, wenn also für ein variables x eine Identität besteht:

$$\Phi(x) = F(x)\, G(x), \tag{9}$$

in der $G(x)$ eine rationale Funktion von x mit rationalen Zahlkoeffizienten bedeutet, deren Nenner durch $F(x)$ nicht teilbar ist. Diese Identität zwischen den drei Funktionen bleibt nun auch für den Bereich von p richtig, wie aus dem a. S. 46 unten bewiesenen Satze unmittelbar folgt; denn jene Gleichung besteht nur dann, wenn die rationalen Zahlkoeffizienten der entsprechenden Potenzen von x links und rechts einander gleich werden. Ersetzt man nun in der aus (9) folgenden Gleichung für den Bereich von p

$$\Phi(x) = F(x)\, G(x) \qquad (p) \tag{9a}$$

wieder x durch die p-adische Reihe α in (6b), so geht sie in eine Gleichung für den Bereich des zu α gehörigen Primteilers $\mathfrak{p}$ über; beachtet man ferner, daß $F(\alpha)$ für den Bereich von $\mathfrak{p}$ gleich Null ist, so ergibt sich auch für den Bereich dieses Primdivisors:

$$\Phi(\alpha) = \varphi(g(\alpha), h(\alpha), \cdots k(\alpha)) = \varphi(\beta, \gamma, \cdots \delta) = 0 \qquad (\mathfrak{p}), \tag{9b}$$

und damit ist der erste Teil unserer Behauptung bewiesen.

Besteht nun umgekehrt für die Zahlen $\beta, \gamma, \ldots \delta$ eine rationale Gleichung mit rationalen Koeffizienten für den Bereich von $\mathfrak{p}$

$$\varphi(\beta, \gamma, \cdots \delta) = \varphi(g(\alpha), h(\alpha), \cdots k(\alpha)) = \Phi(\alpha) = 0 \qquad (\mathfrak{p}),$$

so haben die beiden rationalen Gleichungen mit rationalen Zahlkoeffizienten:

$$\Phi(x) = 0, \quad F(x) = 0 \qquad (p)$$

eine gemeinsame Wurzel $x = \alpha$, d. h. jene beiden Funktionen $\Phi(x)$ und $F(x)$ besitzen für den Bereich von p einen größten gemeinsamen Teiler, welcher, da er durch das Euklidische Verfahren, d. h. auf rationalem Wege aus $F(x)$ und $\Phi(x)$ gefunden wird, ebenfalls rationale Zahlkoeffizienten besitzt. Nun kann aber $F(x)$ auch für den Bereich von p nicht in Faktoren niedrigeren Grades mit rationalen Koeffizienten zerfallen, da aus einer solchen Zerlegungsgleichung für den Bereich von p:

$$F(x) = f(x)\, g(x) \qquad (p)$$

nach dem soeben erwähnten Satze dieselbe Zerlegung der Größe nach folgen müßte, was mit der Voraussetzung der Unzerlegbarkeit von $F(x)$ im Widerspruch stehen würde. Also muß $\Phi(x)$ für den Bereich von p durch $F(x)$ teilbar sein, und die Gleichung

$$\Phi(x) = F(x)\, G(x) \qquad (p), \tag{10}$$

in welcher $F(x)$ ebenfalls rationale Koeffizienten besitzt, bleibt wieder

richtig, wenn man sie nicht für den Bereich von p, sondern ihrer Größe nach betrachtet. Ersetzt man nun in der so sich ergebenden Gleichung:

$$(10a) \qquad \Phi(x) = F(x)\, G(x)$$

wieder x durch α, so ergibt sich, daß auch der Größe nach:

$$\Phi(\alpha) = \varphi(g(\alpha), h(\alpha), \cdots k(\alpha)) = \varphi(\beta, \gamma, \cdots \delta) = 0$$

ist, und damit ist unser Theorem vollständig bewiesen.

Eine rationale ganzzahlige Gleichung für die Zahlen $\beta_1, \gamma_1, \ldots \delta_1$ eines Körpers n^{ter} Ordnung $K(\alpha_1)$

$$(11) \qquad \varphi(\beta_1, \gamma_1, \cdots \delta_1) = \varphi(g(\alpha_1), h(\alpha_1), \cdots k(\alpha_1)) = \Phi(\alpha_1) = 0$$

besteht nach dem soeben bewiesenen Satze dann und nur dann der Größe nach, oder für den Bereich von p, wenn die rationale Funktion $\Phi(x)$ durch die irreduktible Funktion $F(x)$ teilbar ist, welche die linke Seite der Grundgleichung (1) bildet. Substituieren wir nun in die hiernach bestehende Gleichung:

$$\Phi(x) = F(x)\, G(x)$$

eine der n Wurzeln, welche diese Grundgleichung der Größe nach hat, oder eine der n Wurzeln, welche sie für den Bereich von p besitzt, so wird die rechte also auch die linke Seite von (11) gleich Null. Durch die Substitution einer solchen Wurzel werden aber die Zahlen

$$\beta_i = g(\alpha_i), \quad \gamma_i = h(\alpha_i), \quad \cdots \quad \delta_i = k(\alpha_i)$$

die zu $\beta_1, \gamma_1, \ldots \delta_1$ konjugierten Zahlen des zu $K(\alpha_1)$ konjugierten Körpers $K(\alpha_i)$. Hiernach ergibt sich aus der Gleichung (11) der folgende wichtige Satz:

Jede rationale Gleichung mit rationalen Koeffizienten

$$\varphi(\beta_1, \gamma_1, \cdots \delta_1) = 0 \quad (p) \qquad (\text{oder } \varphi(\beta_1, \gamma_1, \cdots \delta_1) = 0),$$

welche für den Bereich von p (oder der Größe nach) zwischen algebraischen Zahlen des Körpers $K(\alpha_1)$ besteht, bleibt richtig, wenn man diese Gleichung ihrer Größe nach (für den Bereich von p) betrachtet, und sie bleibt ferner richtig, wenn man die algebraischen Zahlen durch ihre n konjugierten ersetzt.

§ 2. Die Galoisschen Körper. Untersuchung der Zahlen eines Galoisschen Körpers nach ihrer Größe und für den Bereich einer Primzahl p.

Aus dem im vorigen Paragraphen bewiesenen Satze leite ich nun ein sehr merkwürdiges Theorem her, welches ich aber zunächst nur für den wichtigsten Fall aufstellen und beweisen will, daß die durch die n Wurzeln $\alpha = \alpha_1, \alpha_2, \ldots \alpha_n$ der irreduktiblen Grundgleichung:

(1) $$F(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n) = 0$$

definierten konjugierten Körper

(1a) $$K(\alpha_1), K(\alpha_2), \dots K(\alpha_n)$$

untereinander identisch sind. In diesem Falle, auf den der allgemeinste leicht zurückgeführt werden wird, nenne ich den durch jede der n Wurzeln konstituierten Körper einen Galoisschen Körper. In einem solchen Bereiche herrschen sehr viel einfachere algebraische und arithmetische Gesetze, und der große Fortschritt, den die höhere Algebra sowohl als die höhere Arithmetik dem genialen der Wissenschaft leider viel zu früh, im Alter von kaum 20 Jahren, entrissenen Mathematiker Evariste Galois (gest. 1832) verdankt, beruht im wesentlichen darauf, daß er gelehrt hat, die Untersuchung der allgemeinsten Körper auf die Betrachtung dieser Galoisschen Körper zurückzuführen. Im folgenden wird deshalb auch die Theorie des Galoisschen Körpers an die Spitze der eingehenderen arithmetischen Untersuchung gestellt werden, und daher sollen schon hier die wichtigsten algebraischen und arithmetischen Eigenschaften dieser Körper kurz erörtert werden.

Soll eine Wurzel α_1 der irreduktiblen Gleichung (1) einen Galoisschen Körper definieren, so müssen alle $n - 1$ konjugierten Wurzeln $\alpha_2, \alpha_3, \dots \alpha_n$ dem Körper $K(\alpha_1)$ angehören, also rationale ganzzahlige Funktionen von α_1 sein. Diese notwendige Bedingung ist nun auch hinreichend, damit $K(\alpha_1)$ ein Galoisscher Körper ist. Ist nämlich z. B. α_i eine rationale ganzzahlige Funktion von α_1, so gilt dasselbe von jeder Zahl $\psi(\alpha_i)$ des Körpers $K(\alpha_i)$, und da beide Körper vom n^{ten} Grade sind, so sind sie identisch. Da somit auch α_1 zu $K(\alpha_i)$ gehört, so ist dann auch α_1 durch α_i rational und ganzzahlig ausdrückbar.

> Eine irreduktible Gleichung, deren sämtliche Wurzeln durch eine beliebige unter ihnen rational und ganzzahlig ausdrückbar sind, soll eine Galoissche Gleichung genannt werden.

Hiernach ist also $K(\alpha_1)$ dann und nur dann ein Galoisscher Körper, wenn die ihn definierende Gleichung (1) eine Galoissche Gleichung ist. Ist ferner β_1 irgend eine primitive Zahl von $K(\alpha_1)$, so ist $K(\beta_1) = K(\alpha_1)$ auch ein Galoisscher Körper, also muß auch die β_1 definierende Gleichung eine Galoissche Gleichung sein.

> Ein Körper $K(\alpha_1)$ ist also dann und nur dann ein Galoisscher Körper, wenn jede ihrer primitiven Zahlen einer Galoisschen Gleichung genügt.

Ein Galoisscher Körper wird z. B. durch die irreduktible Gleichung des $\varphi(p-1)^{\text{ten}}$ Grades

$$g(x) = (x - \overline{\omega}_1)(x - \overline{\omega}_2) \ldots (x - \overline{\omega}^{(\sigma)}) = 0$$

definiert, welcher, wie in (4) a. S. 84 angegeben wurde, die $\sigma = \varphi(p-1)$ primitiven $(p-1)^{\text{ten}}$ Wurzeln der Einheit genügen; ist nämlich $\overline{\omega}$ irgend eine unter ihnen, so bestehen ja die $\varphi(p-1)$ Gleichungen:

$$\overline{\omega}_k = \overline{\omega}^{k'} \qquad (k = 1, 2, \cdots \sigma)$$

wo k' die Reihe der $\varphi(p-1)$ zu $p-1$ teilerfremden Zahlen durchläuft.

Ich will nun weiter einen durch eine irreduktible Gleichung n^{ten} Grades

$$F(x) = 0$$

definierten Körper $K(\alpha_1)$ einen Galoisschen Körper für den Bereich der Primzahl p nennen, wenn seine konjugierten $K(\alpha_2), \ldots K(\alpha_n)$ für den Bereich von p mit $K(\alpha_1)$ identisch sind, und ebenso soll eine irreduktible Gleichung eine Galoissche Gleichung für den Bereich dieser Primzahl heißen, wenn ihre Wurzeln für den Bereich von p rationale ganzzahlige Funktionen von einer unter ihnen sind. Dann gilt der wichtige Satz:

> Ein Körper ist dann und nur dann für den Bereich von p ein Galoisscher Körper, wenn ihm die gleiche Eigenschaft der Größe nach zukommt, und das Entsprechende gilt für die Galoisschen Gleichungen.

In der Tat, sei $K(\alpha_1)$ zunächst der Größe nach ein Galoisscher Körper; dann bestehen für die n konjugierten Zahlen $\alpha_1, \alpha_2, \ldots \alpha_n$ der Größe nach n rationale Gleichungen mit rationalen Koeffizienten:

(2) $$\alpha_1 = \alpha_1, \quad \alpha_2 = \varphi_2(\alpha_1), \ldots \alpha_n = \varphi_n(\alpha_1).$$

Es werden nun die n Wurzeln derselben Grundgleichung (1) für den Bereich von p vorläufig durch

(2a) $$\overline{\alpha}_1, \overline{\alpha}_2, \ldots \overline{\alpha}_n$$

bezeichnet; dann behaupte ich, daß diese stets so geordnet werden können, daß sie für den Bereich von p durch dieselben Gleichungen (2) miteinander zusammenhängen, wie die der n Zahlen $\alpha_1, \alpha_2, \ldots \alpha_n$. Es sei nämlich wieder

(3) $$\sum \varepsilon_\lambda^{(1)} \pi^\lambda$$

eine konvergente p-adische Reihe, welche ihrer Größe nach die Wurzel α_1, und für den Bereich von p eine beliebige unter den n p-adischen Wurzeln (2a) derselben Gleichung darstellt; ich will diese letztere dann auch die erste unter den Wurzeln (2a) nennen und jetzt ebenfalls durch α_1 bezeichnen. Dann soll die Reihe (3) wieder die p-adische Darstellung der ersten Wurzel der Grundgleichung genannt werden.

Substituiert man nun diese Reihe für α_1 in die n rationalen Funktionen $\varphi_i(\alpha_1)$ auf der rechten Seite von (2), so erhalten wir n konvergente p-adische Reihen:

$$(4)\qquad \begin{aligned} \alpha_1 &= \quad \alpha_1 \quad = \sum \varepsilon_\lambda^{(1)} \pi^\lambda, \\ \alpha_2 &= \varphi_2(\alpha_1) = \sum \varepsilon_\lambda^{(2)} \pi^\lambda, \\ &\vdots \\ \alpha_n &= \varphi_n(\alpha_1) = \sum \varepsilon_\lambda^{(n)} \pi^\lambda, \end{aligned}$$

welche wegen (2) der Größe nach die n verschiedenen Wurzeln der Grundgleichung darstellen, d. h. es ist der Größe nach erstens allgemein:

$$(5)\qquad F(\alpha_i) = F(\varphi_i(\alpha_1)) = 0,$$

und zweitens besteht für das Differenzenprodukt dieser n Zahlen die ganzzahlige Gleichung:

$$(5\text{a})\qquad \prod_i \prod_k (\alpha_i - \alpha_k) - D = \prod_i \prod_k (\varphi_i(\alpha_1) - \varphi_k(\alpha_1)) - D = 0,$$

wo D die Diskriminante der Grundgleichung bedeutet. Sowohl die n ganzzahligen Gleichungen (5) für die Reihe α_1, als auch die Gleichung (5a) können nun dann und nur dann der Größe nach bestehen, wenn sie auch für den Bereich von p erfüllt sind und umgekehrt. Also folgen aus ihnen für dieselben Reihen die Gleichungen:

$$(6)\qquad F(\varphi_i(\alpha_1)) = 0 \quad (p) \qquad (i = 1, 2, \ldots n)$$

$$(6\text{a})\qquad \prod_i \prod_k (\varphi_i(\alpha_1) - \varphi_k(\alpha_1)) - D = 0 \quad (p).$$

Die n ersten Gleichungen sagen aus, daß die n Reihen $\varphi_i(\alpha_1)$ auch p-adische Wurzeln der Grundgleichung, also gewissen unter den Zahlen $\bar{\alpha}_l$ für den Bereich von p gleich sind. Die letzte Gleichung zeigt, daß diese n Reihen für den Bereich von p voneinander verschieden sind, daß sie also den n Zahlen $\bar{\alpha}_l$, abgesehen von ihrer Reihenfolge, gleich sein müssen. Wären nämlich auch nur zwei unter ihnen für den Bereich von p einander gleich, so würde ihr Differenzenprodukt, also nach (6a) auch die rationale Zahl D, für den Bereich von p gleich Null sein; also wäre D auch der Größe nach Null, was mit der Voraussetzung der Irreduktibilität der Grundgleichung im Widerspruch steht. Damit ist die erste Hälfte unserer Behauptung bewiesen.

Nehmen wir jetzt zweitens an, $K(\bar{\alpha}_1)$ sei für den Bereich von p ein Galoisscher Körper d. h. die n konjugierten Körper

$$K(\bar{\alpha}_1),\ K(\bar{\alpha}_2),\ \ldots\ K(\bar{\alpha}_n)$$

seien für den Bereich von p einander gleich. Dann zeigt man genau ebenso, wie a. S. 333, daß jede der $(n-1)$ konjugierten Zahlen $\bar{\alpha}_2, \ldots \bar{\alpha}_n$ für den Bereich von p einer rationalen Funktion von $\bar{\alpha}_1$ mit gewöhnlichen ganzzahligen Koeffizienten gleich sein, daß also die Grundgleichung (1) und ebenso jede Gleichung der eine primitive Zahl $\bar{\beta}_1$ von $K(\bar{\alpha}_1)$ genügt, eine Galoissche Gleichung für den Bereich von p sein muß. Es seien nun:

$$\bar{\alpha}_1 = \bar{\alpha}_1, \; \bar{\alpha}_2 = \bar{\varphi}_2(\bar{\alpha}_1), \; \ldots \; \bar{\alpha}_n = \bar{\varphi}_n(\bar{\alpha}_1) \quad (p) \tag{7}$$

diese n rationalen Gleichungen für die n Zahlen $\bar{\alpha}_i$. Ist dann wieder:

$$\sum \bar{\varepsilon}_\lambda^{(1)} \pi^\lambda$$

eine konvergente p-adische Reihe, welche für den Bereich von p gleich $\bar{\alpha}_1$ ist, während sie der Größe nach gegen eine der n Gleichungswurzeln (2) etwa gegen α_1 konvergiert, so ergeben sich durch die Substitution jener Reihe für $\bar{\alpha}_1$ in (7) n Gleichungen für $\bar{\alpha}_1, \ldots \bar{\alpha}_n$:

$$\bar{\alpha}_i = \sum \bar{\varepsilon}_\lambda^{(i)} \pi^\lambda \qquad (i = 1, 2, \ldots n), \tag{7a}$$

und diese n Reihen genügen nun für den Bereich von p den $(n+1)$ Gleichungen:

$$F(\bar{\alpha}_i) = F(\bar{\varphi}_i(\bar{\alpha}_1)) = 0 \quad (p) \qquad (i=1, 2, \ldots n)$$

$$\prod_i \prod_k (\bar{\alpha}_i - \bar{\alpha}_k) - D = \prod_i \prod_k (\bar{\varphi}_i(\bar{\alpha}_1) - \bar{\varphi}_k(\bar{\alpha}_1)) - D = 0 \quad (p). \tag{7b}$$

Da nun diese rationalen ganzzahligen Gleichungen für $\bar{\alpha}_1$ wieder nur dann für den Bereich von p bestehen können, wenn sie auch ihrer Größe nach erfüllt sind, so folgt aus ihnen genau wie vorher, daß die n Reihen $\sum \bar{\varepsilon}_\lambda^{(i)} \pi^\lambda$ in (7^a) ihrer Größe nach den n Gleichungswurzeln $\alpha_1, \alpha_2, \ldots \alpha_n$, abgesehen von ihrer Reihenfolge, gleich sind, und damit ist der Beweis unseres Theoremes vollständig erbracht.

Ist

$$\sum_\lambda \varepsilon_\lambda^{(1)} \pi^\lambda \tag{8}$$

eine konvergente p-adische Reihe, welche ihrer Größe nach gegen α_1 und für den Bereich von p gegen eine beliebig aber fest gewählte p-adische Wurzel der Grundgleichung konvergiert, so stellen die in (4) gefundenen Reihen

$$\sum \varepsilon_\lambda^{(i)} \pi^\lambda \qquad (i=1, 2, \ldots n) \tag{8a}$$

der Größe nach die reellen oder komplexen Zahlen $\alpha_1, \alpha_2, \ldots \alpha_n$ dar, während sie für den Bereich von p gegen die n p-adischen Wurzeln $\bar{\alpha}_1, \bar{\alpha}_2, \ldots \bar{\alpha}_n$ in einer ganz bestimmten Reihenfolge konvergieren. In

dieser Ordnung sollen die n p-adischen Wurzeln der Grundgleichung von jetzt an ebenfalls durch

$$\alpha_1, \alpha_2, \ldots \alpha_n$$

bezeichnet werden, und es soll allgemein

$$\alpha_i = \sum \varepsilon_\lambda^{(i)} \pi^\lambda$$

die p-adische Darstellung der i^{ten} Wurzel unserer Gleichung $F(x) = 0$ genannt werden. Da man die p-adische Wurzel, welche die erste Reihe (8) darstellen soll, unter den n p-adischen Wurzeln $\bar{\alpha}_1, \bar{\alpha}_2, \ldots \bar{\alpha}_n$ beliebig auswählen kann, so gibt es genau n, aber auch nur n solche p-adische Darstellungen (8a) jener n Gleichungswurzeln, und damit auch stets n und nur n Zuordnungen der Wurzeln

$$\alpha_1, \alpha_2, \ldots \alpha_n \quad \text{und} \quad \bar{\alpha}_1, \bar{\alpha}_2, \ldots \bar{\alpha}_n.$$

Welche unter ihnen man den weiteren Betrachtungen zugrunde legt, ist gleichgültig, da, wie gleich bewiesen werden soll, die Gleichungen (6) und (6a), welche zwischen ihnen der Größe nach und für den Bereich von p bestehen, und alle anderen rationalen ganzzahligen Gleichungen, welche ja eine Folge von diesen sind, bei jeder dieser n Zuordnungen dieselben sind. Wir denken uns von jetzt an eine dieser Zuordnungen beliebig aber fest ausgewählt, und während der ganzen weiteren Untersuchung beibehalten.

Angenommen nun, zwischen den n Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_n$ einer Galoisschen Gleichung besteht eine rationale Gleichung:

$$\varphi(\alpha_1, \alpha_2, \ldots \alpha_n) = 0 \tag{9}$$

mit gewöhnlichen rationalen Zahlkoeffizienten, so bleibt sie nach dem a. S. 330 bewiesenen Satze auch für den Bereich einer jeden beliebigen Primzahl p richtig, und umgekehrt ergibt sich aus dem Bestehen einer solchen Gleichung für den Bereich irgend einer Primzahl p ihre Richtigkeit der Größe nach und für jede andere Primzahl q. So erhält man das Fundamentaltheorem, auf welches bereits im Anfang dieses Paragraphen hingewiesen wurde:

Ist

$$F(x) = 0$$

eine beliebige Galoissche Gleichung des n^{ten} Grades, so kann man ihre n Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_n$ stets in konvergente p-adische Reihen so entwickeln, daß diese sowohl ihrer Größe nach als auch für den Bereich von p jene Gleichung befriedigen, und daß ferner jede rationale Gleichung:

$$\varphi(\alpha_1, \alpha_2, \ldots \alpha_n) = 0$$

mit rationalen Koeffizienten, welche der Größe nach zwischen ihnen besteht, auch für den Bereich von p erfüllt ist, und umgekehrt.

Ersetzt man in den $(n+1)$ sowohl der Größe nach als auch für den Bereich von p gültigen Gleichungen:

$$(10) \qquad F(\varphi_i(\alpha_1)) = 0, \quad \prod_i \prod_k (\varphi_i(\alpha_1) - \varphi_k(\alpha_1)) - D = 0$$

α_1 der Reihe nach durch die n konjugierten Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_n$, so bleiben sie nach dem a. S. 332 bewiesenen Satze bestehen, und die so sich ergebenden Gleichungen:

$$(10\text{a}) \qquad F(\varphi_i(\alpha_l)) = 0, \quad \prod \prod (\varphi_i(\alpha_l) - \varphi_k(\alpha_l)) - D = 0$$

zeigen, daß die n Zahlen:

$$\alpha_l, \ \varphi_2(\alpha_l), \ldots \varphi_n(\alpha_l)$$

sowohl der Größe nach als auch für den Bereich von p n voneinander verschiedene Wurzeln der Grundgleichung sind, daß sie sich also von den Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_n$ nur durch ihre Reihenfolge unterscheiden. Es ist also z. B. der Größe nach:

$$(10\text{b}) \qquad \varphi_2(\alpha_l) = \alpha_m,$$

und nach dem a. vor. S. unten bewiesenen Satze bleibt jede solche rationale Gleichung zwischen je zwei Wurzeln auch für den Bereich von p richtig.

Vertauscht man also in den n Wurzeln:

$$\alpha_1 = \alpha_1, \ \alpha_2 = \varphi_2(\alpha_1), \ldots \alpha_n = \varphi_n(\alpha_1),$$

α_1 der Reihe nach mit $\alpha_2, \alpha_3, \ldots \alpha_n$, so erleiden diese n Wurzeln jedesmal eine ganz bestimmte Permutation, und zwar stets dieselbe, sowohl der Größe nach als auch für den Bereich der Primzahl p.

Es seien

$$(11) \qquad \begin{aligned} \pi_0 &= (\alpha_1, \ \alpha_2, \ \alpha_3, \ldots \alpha_n) \\ \pi_1 &= (\alpha_{1'}, \ \alpha_{2'}, \ \alpha_{3'}, \ldots \alpha_{n'}) \\ &\vdots \\ \pi_{n-1} &= (\alpha_{1(n-1)}, \ \alpha_{2(n-1)}, \ \alpha_{3(n-1)}, \ldots \alpha_{n(n-1)}) \end{aligned}$$

jene n Permutationen; dann sind allgemein die bei π_i auftretenden Indizes

$$1^{(i)}, 2^{(i)}, \ldots n^{(i)}$$

die n Zahlen $1, 2, \ldots n$ in einer bestimmten Vertauschung, und zwar ist speziell $1^{(i)} = i$.

Diese n Permutationen bilden eine Gruppe; sie haben nämlich die Eigenschaft, daß zwei hintereinander angewandte Permutationen π_i

und π_k wieder eine Permutation π_l aus der Reihe (11) ergeben, daß also stets eine Gleichung:

$$\pi_i \pi_k = \pi_l$$

besteht. In der Tat entsprechen π_i und π_k bzw. der Vertauschung von α_1 mit α_i und von α_1 mit α_k. Da bei der zweiten Vertauschung jede der n Wurzeln sich mit einer anderen vertauscht, so geht bei π_k α_i in eine ganz bestimmte andere Wurzel α_l über. Also entspricht der sukzessiven Anwendung von π_i und π_k die Verwandlung von α_1 in α_i und hierauf die Verwandlung von α_i in α_l, oder was dasselbe ist, die Überführung von α_1 in α_l; also stimmt die Permutation $\pi_i \pi_k$ mit π_l überein. Die n Permutationen (11) bilden somit wirklich eine Gruppe, welche die Gruppe des Galoisschen Körpers $K(\alpha)$ genannt wird.

Jede rationale Gleichung mit rationalen Koeffizienten

$$\varphi(\alpha_1, \alpha_2, \ldots \alpha_n) = 0, \tag{12}$$

welche zwischen den n Wurzeln α der Größe nach besteht, bleibt auch für den Bereich von p gültig und umgekehrt; nach dem a. S. 332 bewiesenen Satze bleibt sie aber auch bestehen, wenn man alle Wurzeln durch eine unter ihnen, etwa durch α_1 ausdrückt, und dann α_1 der Reihe nach durch $\alpha_2, \alpha_3, \ldots \alpha_n$ ersetzt. Aus jener einen Gleichung ergeben sich also die folgenden $2n$ anderen:

$$\varphi(\alpha_{1(k)}, \alpha_{2(k)}, \ldots \alpha_{n(k)}) = 0 \quad (p), \qquad \varphi(\alpha_{1(k)}, \ldots \alpha_{n(k)}) = 0 \tag{12a}$$
$$(k = 0, 1, \cdots n-1).$$

Eine jede rationale Gleichung mit rationalen Koeffizienten, welche zwischen den n Wurzeln einer Galoisschen Gleichung der Größe nach oder für den Bereich einer beliebigen Primzahl besteht, bleibt sowohl in dem einen als auch in dem anderen Sinne richtig, wenn man auf die n Wurzeln alle n Permutationen der zugehörigen Galoisschen Gruppe anwendet.

Ordnet man der ersten Wurzel α_1, welche die Grundgleichung der Größe nach besitzt, einmal die p-adische Wurzel $\bar{\alpha}_1$ ein anderes Mal eine andere p-adische Wurzel $\bar{\alpha}_i$ derselben Grundgleichung für den Bereich von p zu, so ergeben sich für die p-adischen Entwicklungen der n Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_n$ das eine Mal die Reihen $\bar{\alpha}_1, \bar{\alpha}_2, \ldots \bar{\alpha}_n$, das andere Mal dieselben Reihen aber in der Permutation

$$\pi_i = (\bar{\alpha}_{1(i)}, \bar{\alpha}_{2(i)}, \ldots \bar{\alpha}_{n(i)}),$$

welche sich aus der ersten durch die Substitution von $\bar{\alpha}_i$ an der Stelle von $\bar{\alpha}_1$ ergibt. Macht man dieselbe Substitution in den n p-adischen Gleichungen, welche nach dem soeben bewiesenen Satze aus dem Bestehen einer Gleichung:

$$\varphi(\bar{\alpha}_1, \bar{\alpha}_2, \ldots \bar{\alpha}_n) = 0 \quad (p)$$

zwischen den n p-adischen Wurzeln der Grundgleichung durch die Permutationen $\pi_0, \pi_1, \ldots \pi_{n-1}$ der Galoisschen Gruppe folgen, und beachtet dabei, daß die dann sich ergebenden Permutationen $(\pi_i\pi_0, \pi_i\pi_1, \ldots \pi_i\pi_{n-1})$ abgesehen von der Reihenfolge mit den vorigen übereinstimmen, so erkennt man

> daß die $2n$ Gleichungen (12a), welche aus einer unter ihnen mit Notwendigkeit folgen, von der Art der p-adischen Entwicklung der ersten Wurzel α_1 ganz unabhängig sind, da man bei jeder der n möglichen Entwicklungen dieselben n Gleichungen für den Bereich von p erhält.

§ 3. Untersuchung der Zahlen eines beliebigen Körpers nach ihrer Größe und für den Bereich von p.

Die im vorigen Abschnitte für Galoissche Körper gefundenen Resultate können nun leicht auch für ganz beliebige algebraische Körper begründet werden. Hierzu führt der jetzt zu gebende Nachweis der Tatsache, daß jeder algebraische Körper entweder selbst ein Galoisscher Körper, oder ein Unterkörper eines solchen ist, daß also jede algebraische Zahl β_1 als eine primitive oder als eine nicht primitive Zahl eines Galoisschen Körpers angesehen werden kann. Da nun alle Zahlen β_1 eines Galoisschen Körpers $K(\alpha_1)$ nebst ihren konjugierten nach den Ergebnissen des vorigen Paragraphen so in konvergierende p-adische Reihen entwickelt werden können, daß jede zwischen ihnen der Größe nach bestehende Gleichung auch für den Bereich von p erfüllt ist und umgekehrt, so ist damit der verlangte Nachweis auch für beliebige algebraische Zahlen erbracht. Ich will daher jetzt noch den soeben erwähnten algebraischen Satz beweisen.

Es sei

(1) $$f(x) = (x-\beta_1)(x-\beta_2)\ldots(x-\beta_\nu) = 0$$

eine beliebige irreduktible Gleichung ν^{ten} Grades mit rationalen Zahlkoeffizienten, deren Wurzeln keinen Galoisschen Körper konstituieren mögen. Dann betrachte ich den Körper:

$$K(\beta_1, \beta_2, \ldots \beta_\nu),$$

welcher durch die ν konjugierten Zahlen $\beta_1, \beta_2, \ldots \beta_\nu$ zusammen konstituiert, also durch alle rationalen Funktionen dieser ν Zahlen mit rationalen Zahlkoeffizienten gebildet wird. Ich behaupte nun, daß dieser ein Galoisscher Körper ist, welcher jeden der ν konjugierten Körper $K(\beta_i)$ als Unterkörper enthält.

Zunächst erkennt man leicht, daß in dem durch die ν Zahlen

$$\beta_1, \beta_2, \ldots \beta_\nu$$

konstituierten Körper auf unendlich viele Arten eine primitive Zahl α_1 so ausgewählt werden kann, daß alle Zahlen desselben durch α_1 rational darstellbar sind, daß also

$$K(\beta_1, \beta_2, \ldots \beta_\nu) = K(\alpha_1)$$

ist. In der Tat, sei zunächst

(2) . $$\bar{\alpha}_1 = x_1\beta_1 + x_2\beta_2 + \cdots + x_\nu\beta_\nu$$

eine homogene lineare Funktion der ν konjugierten Zahlen β_i mit den unbestimmten Koeffizienten x_i, und es mögen:

(2a) $$\bar{\alpha}_k = x_1\beta_{1(k)} + x_2\beta_{2(k)} + \cdots + x_\nu\beta_{\nu(k)} \qquad (k=1, 2, \ldots \nu!)$$

die $\nu!$ Formen sein, welche man aus $\bar{\alpha}_1$ erhält, wenn man die ν Elemente β_i auf alle $\nu!$ möglichen Arten permutiert. Diese Formen sind für unbestimmte x_i alle voneinander verschieden, weil von den Wurzeln $\beta_1, \beta_2, \ldots \beta_\nu$ keine zwei einander gleich sind. Dann ist jede symmetrische Funktion:

$$S(\bar{\alpha}_1, \bar{\alpha}_2, \ldots \bar{\alpha}_{\nu!})$$

dieser $\nu!$ Formen $\bar{\alpha}_k$ eine symmetrische Funktion auch von $\beta_1, \beta_2, \ldots \beta_\nu$, weil durch jede Vertauschung der β_i untereinander nur die Formen $\bar{\alpha}_k$ permutiert werden; jede solche Funktion ist also eine rationale Funktion der Unbestimmten $x_1, \ldots x_\nu$ mit rationalen Zahlkoeffizienten. Speziell ist die Diskriminante

(3) $$D(\bar{\alpha}_1, \ldots \bar{\alpha}_{\nu!}) = \prod_i \prod_k (\bar{\alpha}_i - \bar{\alpha}_k)$$

dieser $\nu!$ Formen eine ganze homogene Form der $x_1, \ldots x_\nu$ mit rationalen Zahlkoeffizienten, welche für unbestimmte x_k von Null verschieden ist, weil nach der soeben über die β_i gemachten Bemerkung keine von den Differenzen $\bar{\alpha}_i - \bar{\alpha}_k$ für unbestimmte x_h Null sein kann.

Da somit $D(\bar{\alpha}_1, \bar{\alpha}_2, \ldots \bar{\alpha}_{\nu!})$ eine ganze homogene Form der Unbestimmten $x_1, x_2, \ldots x_\nu$ ist, welche nicht identisch verschwindet, so kann man bekanntlich*) die Größen x_i auf unendlich viele Weisen ganzzahlig so bestimmen, daß diese Diskriminante ebenfalls von Null verschieden wird. Es sei

(4) $$x_1 = a_1, \ x_2 = a_2, \ldots x_\nu = a_\nu$$

eine solche Bestimmung, und

*) Vgl. z. B. Weber Algebra. II. Aufl. Bd. I. § 48.

$$
(5)\quad
\begin{aligned}
\alpha_1 &= a_1\beta_1 + a_2\beta_2 + \cdots + a_\nu\beta_\nu\\
\alpha_2 &= a_1\beta_{1(2)} + a_2\beta_{2(2)} + \cdots + a_\nu\beta_{\nu(2)}\\
&\vdots\\
\alpha_{\nu!} &= a_1\beta_{1(\nu!)} + a_2\beta_{2(\nu!)} + \cdots + a_\nu\beta_{\nu(\nu!)}
\end{aligned}
$$

seien die $\nu!$ Zahlen des Körpers $K(\beta_1, \beta_2, \ldots \beta_\nu)$, welche durch diese Substitution (4) aus $\bar{\alpha}_1, \ldots \bar{\alpha}_{\nu!}$ hervorgehen. Dann sind auch sie alle voneinander verschieden, und sie genügen zusammen einer Gleichung des $(\nu!)^{\text{ten}}$ Grades:

$$
(6)\qquad G(t) = (t-\alpha_1)(t-\alpha_2)\ldots(t-\alpha_{\nu!}) = 0,
$$

deren Koeffizienten als symmetrische Funktionen der α_k, also auch der $\beta_1, \beta_2, \ldots \beta_\nu$, gewöhnliche rationale Zahlen sind.

Ich behaupte nun, daß die so gefundene Zahl α_1 eine primitive Zahl des Körpers $K(\beta_1, \beta_2, \ldots \beta_\nu)$, d. h. so beschaffen ist, daß jede andere Zahl $\Theta(\beta_1, \beta_2, \ldots \beta_\nu)$ dieses Körpers durch α_1 rational ausdrückbar ist. In der Tat, seien:

$$
\Theta_1, \Theta_2, \ldots \Theta_{\nu!}
$$

die Werte, welche $\Theta(\beta_1, \beta_2, \ldots \beta_\nu)$ bei allen $\nu!$ Permutationen der ν Zahlen β_i erhält, so ist

$$
(7)\qquad \chi(t) = G(t)\left\{\frac{\Theta_1}{t-\alpha_1} + \frac{\Theta_2}{t-\alpha_2} + \cdots + \frac{\Theta_{\nu!}}{t-\alpha_{\nu!}}\right\}
$$

eine ganze rationale Funktion der Variablen t mit gewöhnlichen rationalen Zahlenkoeffizienten, da sich ja die im Nenner stehenden Linearfaktoren gegen $G(t)$ fortheben und da $\chi(t)$ symmetrisch in $\beta_1, \beta_2, \ldots \beta_\nu$ ist.

Setzt man in dieser Gleichung $t = \alpha_1$ und beachtet, daß dann alle Produkte $G(\alpha_1)\dfrac{\Theta_i}{t-\alpha_i}$ außer dem ersten verschwinden, während dieses gleich $G'(\alpha_1)\Theta_1$ wird, so ergibt sich die folgende rationale Darstellung der beliebig angenommenen Zahl Θ_1 des Körpers $K(\beta_1, \ldots \beta_\nu)$ durch α_1

$$
\Theta_1 = \frac{\chi(\alpha_1)}{G'(\alpha_1)},
$$

und sie ist nicht etwa unbestimmt, weil

$$
G'(\alpha_1) = \prod_{k=2}^{\nu!}(\alpha_1 - \alpha_k)
$$

sicher von Null verschieden ist. Hieraus folgt, daß wirklich

$$
K(\beta_1, \beta_2, \ldots \beta_\nu) = K(\alpha_1)
$$

ist.

Ich behaupte nun zweitens, daß $K(\alpha_1)$ ein Galoisscher Körper ist, d. h. daß alle zu α_1 konjugierten Zahlen durch α_1 rational darstellbar sind. Es sei nun

$$g(t) = (t - \alpha_1)(t - \alpha_1') \ldots (t - \alpha_1^{(n-1)}) = 0$$

die irreduktible Gleichung, welcher die algebraische Zahl α_1 nebst ihren konjugierten $\alpha_1', \ldots \alpha_1^{(n-1)}$ genügt. Dann haben die beiden Gleichungen $g(t) = 0$ und $G(t) = 0$ in (6) die eine Wurzel α_1 gemeinsam, also müssen sie einen gemeinsamen Teiler besitzen; und da $g(t)$ irreduktibel ist, so muß $G(t)$ durch $g(t)$ teilbar sein. Aus der somit bestehenden Gleichung:

$$G(t) = g(t)\, H(t)$$

folgt nun, daß die zu α_1 konjugierten Zahlen $\alpha_1', \ldots \alpha_1^{(n-1)}$ gewisse unter den Zahlen $\alpha_2, \alpha_3, \ldots \alpha_{\nu!}$ sein müssen. Die Bezeichnung werde so gewählt, daß $\alpha_1, \alpha_2, \ldots \alpha_n$ diese konjugierten Zahlen sind. Da nun jede der Zahlen

$$\alpha_i = a_1 \beta_{1(i)} + a_2 \beta_{2(i)} + \cdots + a_n \beta_{n(i)} \qquad (i = 1, 2, \ldots n)$$

dem Körper $K(\beta_1, \ldots \beta_\nu)$ angehört, und da dieser nach dem soeben geführten Beweise mit $K(\alpha_1)$ übereinstimmt, so folgt, daß

$$K(\alpha_1) = K(\beta_1, \beta_2, \ldots \beta_\nu)$$

wirklich ein Galoisscher Körper ist, unter welchem die ν konjugierten Körper $K(\beta_i)$ als Unterkörper enthalten sind.

Es sei nun β_1 eine beliebige algebraische Zahl ν^{ten} Grades; $\beta_2, \beta_3, \ldots \beta_\nu$ mögen die zu β_1 konjugierten Zahlen bedeuten, und es sei jetzt

$$(8) \qquad f(x) = (x - \beta_1)(x - \beta_2) \ldots (x - \beta_\nu) = 0$$

die irreduktible Gleichung, welcher die Zahlen β_i genügen. Ich betrachte dann den zugehörigen Galoisschen Körper $K(\beta_1, \beta_2, \ldots \beta_\nu)$, dessen Grad n sein möge, und bezeichne durch $\alpha_1, \alpha_2, \ldots \alpha_n$ irgend eine primitive Zahl jenes Körpers und ihre konjugierten: Ich denke mir nun α_1 durch die zugehörige Reihe

$$(9) \qquad \alpha_1 = \sum \varepsilon_\lambda \pi^\lambda,$$

sowohl der Größe nach als auch für den Bereich von p dargestellt. Da nun die ν Zahlen β_i rationale ganzzahlige Funktionen $\psi_i(\alpha_1)$ von α_1 sind, so liefert die Substitution der obigen Reihe (9) für α_1 in die ν Gleichungen:

$$(10) \qquad \beta_1 = \psi_1(\alpha_1),\ \beta_2 = \psi_2(\alpha_1), \ldots, \beta_\nu = \psi_\nu(\alpha_1)$$

ν p-adische Reihen

$$(11) \qquad \beta_i = \sum \delta_\lambda^{(i)} \pi^\lambda \qquad (i = 1, 2, \ldots \nu)$$

für jene Zahlen, welche so beschaffen sind, daß jede zwischen ihnen der Größe nach bestehende rationale ganzzahlige Gleichung auch für den Bereich von p erfüllt ist, und umgekehrt. Da nun $\beta_1, \beta_2, \dots \beta_\nu$ den $(\nu+1)$ rationalen Gleichungen:

$$(12) \qquad f(\beta_i) = 0, \quad \prod_i \prod_k (\beta_i - \beta_k) - D = 0$$

genügen, in welchen D die Diskriminante der Grundgleichung (8) bedeutet, so liefert die Substitution der ν Reihen (11) für $\beta_1, \dots \beta_\nu$ in diese Gleichungen das Resultat, daß dieselben die ν voneinander verschiedenen Wurzeln der Gleichung (8), sowohl der Größe nach als auch für den Bereich von p darstellen. Ist allgemeiner

$$(12\text{a}) \qquad \chi(\beta_1, \beta_2, \dots \beta_\nu) = 0$$

irgend eine rationale ganzzahlige Gleichung zwischen den ν konjugierten Zahlen β_i, so folgt aus demselben Satze, daß diese auch für den Bereich von p erfüllt ist, wenn man für die Zahlen β_i ihre Reihen (11) einsetzt, und daß auch umgekehrt aus dem Bestehen einer solchen Gleichung für den Bereich von p ihre Richtigkeit folgt, wenn man die Zahlen β_i ihrer Größe nach betrachtet.

Substituiert man in die $(\nu+1)$ Gleichungen (12) für die konjugierten Zahlen β_i ihre rationalen Ausdrücke $\psi_i(\alpha_1)$ durch die primitive Zahl α_1 des Galoisschen Körpers $K(\beta_1, \beta_2, \dots \beta_\nu)$ so bleiben die Gleichungen:

$$(13) \qquad f(\psi_i(\alpha_1)) = 0, \quad \prod_i \prod_k (\psi_i(\alpha_1) - \psi_k(\alpha_1)) - D = 0,$$

sowohl der Größe nach, als auch für den Bereich von p richtig, wenn man α_1 mit den n konjugierten Zahlen $\alpha_1, \alpha_2, \dots \alpha_n$ vertauscht; hieraus folgt, daß die Zahlen:

$$\beta_{1(l)} = \psi_1(\alpha_l), \ \beta_{2(l)} = \psi_2(\alpha_l), \ \dots \ \beta_{\nu(l)} = \psi_\nu(\alpha_l)$$

für $l = 1, 2, \dots n$ jedesmal die ν Zahlen $\beta_1, \beta_2, \dots \beta_\nu$ in anderer Reihenfolge sowohl der Größe nach als auch für den Bereich von p darstellen. So ergeben sich n Permutationen dieser ν Wurzeln:

$$(14) \qquad \begin{aligned} \pi_1 &= (\beta_{1'}, \beta_{2'}, \cdots \beta_{\nu'}) \\ \pi_2 &= (\beta_{1''}, \beta_{2''}, \cdots \beta_{\nu''}) \\ &\vdots \\ \pi_n &= (\beta_{1^{(n)}}, \beta_{2^{(n)}}, \cdots \beta_{\nu^{(n)}}), \end{aligned}$$

bei denen die erste $\pi_1 = (1', 2', \cdots \nu')$ die ursprüngliche Anordnung $(1, 2, \dots \nu)$ bedeutet.

Ich behaupte nun:

1) Die so sich ergebenden Permutationen sind dieselben, mag man die Zahlen β_i ihrer Größe nach oder für den Bereich von p betrachten.
2) Die n Permutationen π_i sind alle untereinander verschieden.
3) Sie bilden eine Gruppe, d. h. es ist allgemein $\pi_i \pi_k = \pi_l$.

Ist nämlich z. B. der Größe nach:

$$\beta_{1''} = \psi_1(\alpha_2) = \beta_i = \psi_i(\alpha_1),$$

so besteht zwischen α_1 und α_2 die rationale Gleichung mit rationalen Koeffizienten:

$$\psi_i(\alpha_1) = \psi_1(\alpha_2),$$

und diese bleibt für den Bereich von p richtig, wenn sie der Größe nach erfüllt ist; damit ist der erste Teil unserer Behauptung bewiesen. Wären zweitens etwa die zweite und dritte Permutation der β_i einander gleich, so daß:

$$\beta_{i''} = \beta_{i'''}, \text{ d. h. } \psi_i(\alpha_2) = \psi_i(\alpha_3) \qquad (i = 1, 2, \cdots \nu)$$

ist, so wäre auch:

$$a_1 \beta_{1''} + a_2 \beta_{2''} + \cdots + a_\nu \beta_{\nu''} = a_1 \beta_{1'''} + \cdots + a_\nu \beta_{\nu'''},$$

d. h. es wäre $\alpha_2 = \alpha_3$, während doch α_1 eine primitive Zahl des Galoisschen Körpers $K(\alpha)$ ist. Endlich bilden diese n Vertauschungen π_i eine Gruppe, da sie den n Vertauschungen von α_1 mit den n konjugierten eindeutig zugeordnet sind. Ich nenne sie die Galoissche Gruppe von jedem der ν konjugierten Körper $K(\beta_i)$.

Es möge nun zwischen diesen ν konjugierten Zahlen $\beta_1, \beta_2, \ldots \beta_\nu$ irgend eine rationale ganzzahlige Gleichung:

$$(15) \qquad \psi(\beta_1, \beta_2, \cdots \beta_\nu) = 0$$

der Größe nach oder für den Bereich von p bestehen. Substituiert man dann für die Zahlen β_i ihre rationalen Darstellungen $\psi_i(\alpha_1)$ durch α_1 und vertauscht dann α_1 mit den n konjugierten Zahlen $\alpha_1, \alpha_2, \ldots \alpha_n$, so bleibt diese Gleichung sowohl der Größe nach, als auch für den Bereich von p richtig. Durch diese Vertauschungen erleiden aber die Wurzeln $\beta_1, \beta_2, \ldots \beta_\nu$ die n Permutationen $\pi_1, \pi_2, \ldots \pi_n$ ihrer Galoisschen Gruppe, d. h. aus (15) folgen von selbst die $2n$ Gleichungen:

$$(15\text{a}) \quad \psi(\beta_{1^{(i)}}, \beta_{2^{(i)}}, \cdots \beta_{\nu^{(i)}}) = 0 \quad (p); \qquad \psi(\beta_{1^{(i)}}, \beta_{2^{(i)}}, \cdots \beta_{\nu^{(i)}}) = 0 \quad (i = 1, 2, \cdots n),$$

und man erhält das folgende Schlußresultat:

Man kann alle algebraischen Zahlen stets so in konvergente p-adische Potenzreihen entwickeln, daß jede zwischen ihnen der Größe nach bestehende rationale Gleichung mit rationalen

Zahlkoeffizienten auch für den Bereich von p richtig bleibt und umgekehrt. Ferner bleibt jede solche Gleichung in dem einen wie in dem anderen Sinne bestehen, wenn man auf ihre linke Seite alle Permutationen der zugehörigen Galoisschen Gruppe anwendet.

Jede rationale Gleichung zwischen bestimmten algebraischen Zahlen oder jedes System von solchen Gleichungen liefert einen algebraischen Satz, und umgekehrt kann fast jeder derartige Satz als die Interpretation eines solchen Gleichungsystemes ausgesprochen werden. Ebenso ergibt jedes Gleichungssystem für den Bereich einer reellen Primzahl p eine arithmetische Wahrheit, und umgekehrt ist die ganze Arithmetik der algebraischen Zahlen nichts anderes als die Interpretation aller zwischen jenen Zahlen für den Bereich aller reellen Primzahlen bestehenden Gleichungen. Der soeben gefundene allgemeine Satz zeigt nun, daß jedem algebraischen Satze eine arithmetische Wahrheit entspricht und umgekehrt. Der Ausführung dieses Dualismus bei den speziellen algebraischen Zahlkörpern werden die Untersuchungen des folgenden Bandes zu einem großen Teile gewidmet sein.

— Ende des ersten Bandes. —

Sachregister.

(Die Ziffern bezeichnen die Seite, auf welcher sich das betreffende Wort meistens gesperrt gedruckt findet und erklärt wird.)

Druckfehler.

S. 18,	Z. 11	von oben	statt	„vor und“	lies „vor, und“.
S. 101,	Z. 16	„ „	„	„reelle“	lies „rationale“.
S. 101,	Z. 19	„ „	„	„reellen“	lies „rationalen“.
S. 130,	Z. 7	„ „	„	„mstande“	lies „imstande“.
S. 247,	Z. 9	„ unten	„	(1	lies (1).
S. 253,	Z. 13	„ „	„	$\eta^{(i)})$	lies $(\eta^{(i)})$.
S. 299,	Seitenzahl		statt 29		lies 299.

Druck von B. G. Teubner in Leipzig.

Verlag von B. G. Teubner in Leipzig und Berlin.

Theorie der algebraischen Funktionen einer Variabeln u. ihre Anwendung auf algebraische Kurven und Abelsche Integrale

Von

Dr. Kurt Hensel, Professor der Mathematik an der Universität Marburg a. L., und **Dr. Georg Landsberg,** Professor der Mathematik an der Universität Kiel.

Mit vielen Figuren im Text. [XVI u. 708 S.] gr. 8. 1902. In Leinwand geb. n. *M.* 28.—

Inhalt: I. Teil: Ausbreitung der algebraischen Funktionen auf der Riemannschen Fläche. II. Teil: Der Körper algebraischer Funktionen. III. Teil: Die algebraischen Divisoren und der Riemann-Rochsche Satz. IV. Teil: Die algebraischen Kurven oder Gebilde. V. Teil: Die Klassen algebraischer Gebilde. VI. Teil: Algebraische Relationen zwischen Abelschen Integralen. Anhang. Sachregister.

Das Buch gibt im Sinne der Arbeiten von Weierstraß, Kronecker, Dedekind, H. Weber eine umfassende Behandlung der Theorie der algebraischen Funktionen einer Variabeln auf wesentlich arithmetischer Basis mit Anwendung auf die Abelschen Integrale und algebraischen Kurven. Dabei haben sich die Verfasser bemüht, die ganze Theorie und alle aus ihr abzuleitenden Folgerungen ohne jede sogenannte vereinfachende Voraussetzung zu begründen und nur solche Methoden und Definitionen zu benutzen, welche auf jeden vorgelegten, noch so speziellen Fall anwendbar bleiben, und zwar so, daß die verlangten Rechnungen stets wirklich ausgeführt werden können.

Vorlesungen über Zahlentheorie

Einführung in die Theorie der algebraischen Zahlkörper

Von **Dr. J. Sommer,** Professor an der Technischen Hochschule zu Danzig.

Mit 4 Figuren im Text. [VI u. 361 S.] gr. 8. 1907. In Leinwand geb. n. *M.* 11.—

Seitdem Gauß die Arithmetik durch Aufnahme der komplexen Zahlen $a+b\sqrt{-1}$ erweitert hat, ist eine großartige Theorie der allgemeinen algebraischen Zahlen entstanden, deren Entwicklung vor allem an die Namen Kummer, Dirichlet, Dedekind, Kronecker und einiger rühmlichst bekannten neueren Mathematiker sich knüpft. Mehrfach hat diese Theorie ihr Aussehen stark verändert, und wir besitzen von den berufensten Seiten: Dedekind, Hilbert und Kronecker-Hensel, wie neuerdings von Bachmann zusammenfassende Werke, die den Stoff von verschiedenen Gesichtspunkten aus auffassen. Jedes dieser Werke bedeutet nicht nur in bezug auf den Inhalt, sondern auch in Anbetracht der formalen Abrundung der ganzen Darstellung einen sehr wesentlichen Fortschritt für die allgemeine Zahlentheorie. Da diese aber alle den allgemeinen Fall der Theorie umfassen und für Anfänger schwer zu lesen sind, so dürfte wohl eine Darstellung nützlich sein, die auf möglichst elementare Weise in die Probleme und Tatsachen der Zahlkörpertheorie einführt. Dieser Zweck wird von selbst durch eine spezielle Behandlung der einfachsten, quadratischen und kubischen Zahlkörper erreicht. Zum Studium des vorliegenden Buches sind nur wenige Vorkenntnisse aus der Algebra notwendig. Der Verfasser hat gesucht, überall mit den einfachsten Methoden zum Ziele zu gelangen, und hat sich überhaupt derjenigen Behandlung der Theorie angeschlossen, die ihm als die einfachste erscheint, und die man in den Arbeiten von Hurwitz, Hilbert und Minkowski niedergelegt findet.

N.